IKARUS anti.virus

Benutzerhandbuch

Inhaltsverzeichnis

1 Einleitung **3**

1.1 Über IKARUS Security Software 3

2 Die Installation von IKARUS anti.virus **4**

2.1 Systemvoraussetzungen 4

2.2 Installation von **IKARUS anti.virus** 5

2.3 Installation von der Kommandozeile 12

2.4 Deinstallation von **IKARUS anti.virus** 13

3 Funktionen von IKARUS anti.virus **16**

3.1 Symbole und Anzeigen 16

4 Der Guard - Ihr Sicherheitswächter **18**

5 Das Update von IKARUS anti.virus **20**

6 Der Scan - die Virenprüfung von IKARUS anti.virus **21**

6.1 Die Scan-Einstellungen 23

7 Was tun bei Virenfund - die Quarantäne **25**

7.1 Anzeigen eines Virenfundes 25

7.2 Virenfund beim Scanvorgang 25

7.3 Die Quarantäne 26

8 Anti-SPAM **30**

9 Microsoft-SharePoint-Überwachung **31**

9.1 Leistungsumfang 31

9.2 Installation 32

9.3 Arbeitsweise 32

10 Einstellungen **36**

10.1 Spracheinstellungen 36

10.2 Protokolle 36

10.3 Einstellungen 37

11 Support **41**

11.1 Lizenzschlüssel 42

12 Anhang **44**

12.1 .NET Framework 44

12.2 Personal Firewall 46

12.3 Lizenzrechtliche Bestimmungen 50

1 Einleitung

Vielen Dank, dass Sie sich für **IKARUS anti.virus** von IKARUS Security Software entschieden haben.

IKARUS anti.virus ist der effiziente Virenschutz für Workstations und Server mit Microsoft Betriebssystemen und schützt vor SPAM, Viren, Trojanern, Würmern, Dialern, Maliciouse Codes und vielen anderen Schadprogrammen. Zwei Komponenten sorgen für Sicherheit vor Bedrohungen aus dem Internet: Einerseits ermöglicht **IKARUS anti.virus** die manuelle Suche nach elektronischen Schädlingen, und andererseits läuft der Onlinewächter ”Guard” ständig im Hintergrund und überprüft aller Schreib- und Lesezugriffe.

1.1 Über IKARUS Security Software

IKARUS Security Software GmbH (”**IKARUS**”) ist ein österreichischer Pionier der Softwareindustrie mit Schwerpunkt auf Antivirus und Content-Security. Seit der Gründung im Jahre 1986 entwickelt das Unternehmen Sicherheitslösungen und zählt zu den ersten Antivirenherstellern weltweit.

IKARUS investiert jährlich rund 75 Prozent des Gesamtumsatzes in softwaregebundene Forschung und Entwicklung und steht mit Sicherheitsexperten in verschiedensten Ländern in Kontakt: Täglich tauschen die Experten von **IKARUS** weltweit Vireninformationen mit anderen Forschungszentren aus. Im Mittelpunkt der derzeitigen Forschung stehen Projekte in technischen, rechtlichen und gesellschaftlichen Bereichen: von der formalen Virusdeskription über neue Ansätze durch das Sonderstrafrecht bis hin zu geschlossenen und offenen Datensicherheitssystemen.

Die Produktpalette von **IKARUS** reicht von einfach zu bedienenden, effizienten Sicherheitsprodukten für Heimanwender bis zu umfassenden Sicherheitspaketen zur Absicherungen komplexer Unternehmensnetzwerke: **IKARUS** schützt effektiv und effizient vor Viren, Trojanern, Spyware, SPAM und Malware, die die Sicherheit Ihrer Geräte und Daten gefährden. Professionelle Beratung und kostenloser Support inklusive.

2 Die Installation von IKARUS anti.virus

In diesem Kapitel erfahren Sie, wie man die **IKARUS anti.virus** installiert und erfolgreich in Betrieb nimmt. Jeder Installationsschritt ist mit Bildern dokumentiert und kann 1:1 nachvollzogen werden.

2.1 Systemvoraussetzungen

Damit Sie die **IKARUS anti.virus** problemlos verwenden können, sind folgende Systemvoraussetzungen notwendig:

- Computer mit Intel Pentium oder AMD Prozessor ab 2 GHz
- 1 GB RAM
- mind. 200 MB freier Speicherplatz
- Bildschirmauflösung min. 1024 x 768

Eines der folgenden Betriebssysteme muss auf Ihrem Computer installiert sein:

- Windows XP, Service Pack 2 (32 Bit)
- Windows Vista (32 Bit)
- Windows 7 (32 Bit)
- Windows 2003 (32 Bit)
- Windows Server 2008 (32 Bit)
- Windows 2003 (64 Bit)
- Windows XP, Service Pack 2 (64 Bit)
- Windows Vista (64 Bit)
- Windows 7 (64 Bit)
- Windows Server 2008 (64 Bit)

Achtung: Bitte deinstallieren Sie vor der Installation von **IKARUS anti.virus** andere auf Ihrem PC befindlichen Anti-Virenprogramme und führen Sie danach einen Neustart des Computers durch.

Schließen Sie während des Installationsvorgangs von **IKARUS anti.virus** alle anderen Programme.

Nach der Installation von **IKARUS anti.virus** wird eine schnelle Systemprüfung durchgeführt. Diese dauert durchschnittlich rund 10 Minuten.

Bitte führen Sie diese Systemprüfung nach der Installation auf jeden Fall durch, sie dient der Sicherheit Ihres PCs!

2.2 Installation von IKARUS anti.virus

Legen Sie die Installations-CD in das CD-ROM-Laufwerk Ihres PCs. Wir empfehlen alle anderen Programme vor der Installation zu beenden.

Die Installation startet grundsätzlich automatisch.

Sollte die Installation nicht automatisch starten, öffnen Sie den Windows Explorer und wählen Sie das CD-ROM-Laufwerk aus.

Durch ein Doppelklicken der Datei ”Setup IKARUS anti.virus 2.2.3.exe” starten Sie das Programm.

Schritt 1: Folgen Sie für die Installation von **IKARUS anti.virus** bitte den Anweisungen des Installationsassistenten.

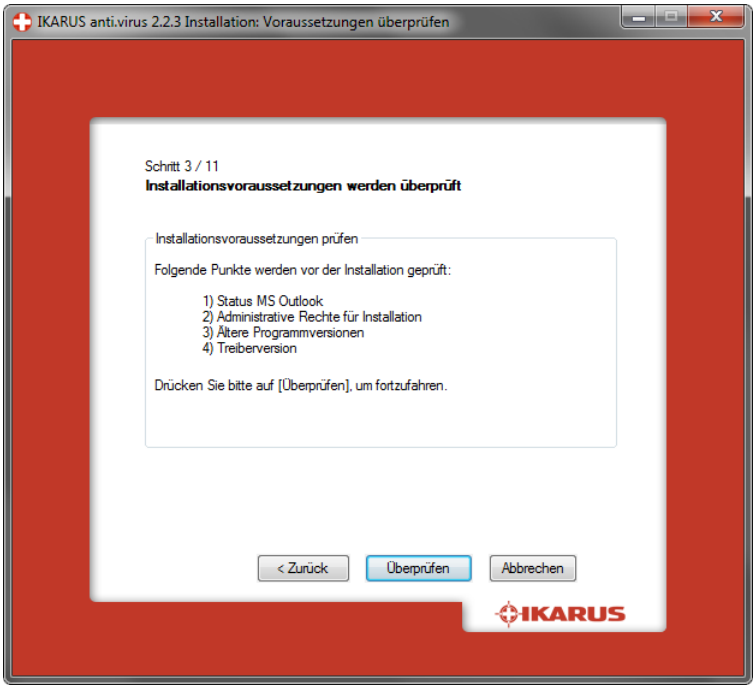
IKARUS anti.virus 2.2.3 Installation
Schritt 1 / 11
Willkommen bei der Installation von IKARUS anti.virus 2.2.3
Der Installations-Assistent wird Sie durch die Installation von IKARUS anti.virus 2.2.3 begleiten.
Es wird empfohlen, vor der Installation alle anderen Programme zu schließen, damit bestimmte Systemdateien ohne Neustart ersetzt werden können.
Wenn Sie alle Programme geschlossen haben, klicken Sie auf [Weiter], um mit der Installation fortzufahren.
Compatible with
Windows 7
Weiter >
Abbrechen
IKARUS

Schritt 2: Akzeptieren Sie bitte die Lizenzbestimmungen von IKARUS, um mit der Installation fortzufahren.

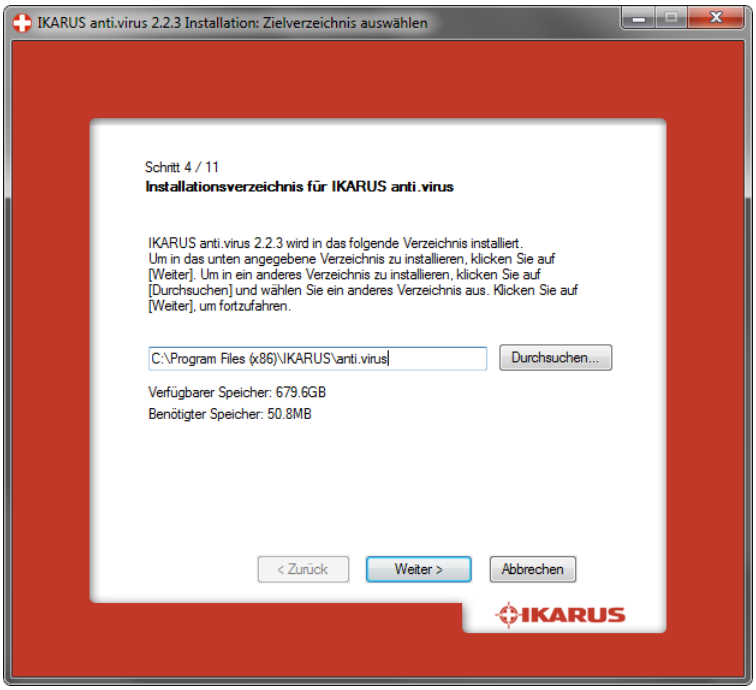
IKARUS anti.virus 2.2.3 Installation: Lizenzbedingungen
Schritt 2 / 11
Lizenzbedingungen
Drücken Sie [Bild-nach-unten], um den Rest des Abkommens zu sehen.
IKARUS SECURITY SOFTWARE LIZENZ- UND WARTUNGSVERTRAG
Lesen Sie bitte diese Vereinbarung sorgfältig durch! Mit Installierung der gelieferten Software anerkennen Sie die untenstehenden Lizenzbedingungen. Sollten Sie damit nicht einverstanden sein, brechen Sie den Installationsvorgang ab und nehmen Sie von der weiteren Verwendung der gelieferten Software Abstand. Eine Verletzung dieser Lizenzbedingungen kann eine Urheberrechtsverletzung sein, die zivil- und strafrechtlich verfolgt wird.
1. Lizenz
1.1. Lizenzgeber ist die IKARUS Security Software GmbH. Gegenstand
Sie müssen die Lizenzbedingungen anerkennen, um IKARUS anti.virus 2.2.3 installieren zu können. Falls Sie alle Bedingungen des Abkommens akzeptieren, klicken Sie auf [Annehmen].
< Zurück
Annehmen
Abbrechen
IKARUS

Schritt 3: IKARUS anti.virus überprüft, ob das E-Mail-Programm beendet ist, alle Rechte zur Installation vorhanden sind und ob eine ältere Version von **IKARUS anti.virus** installiert ist.

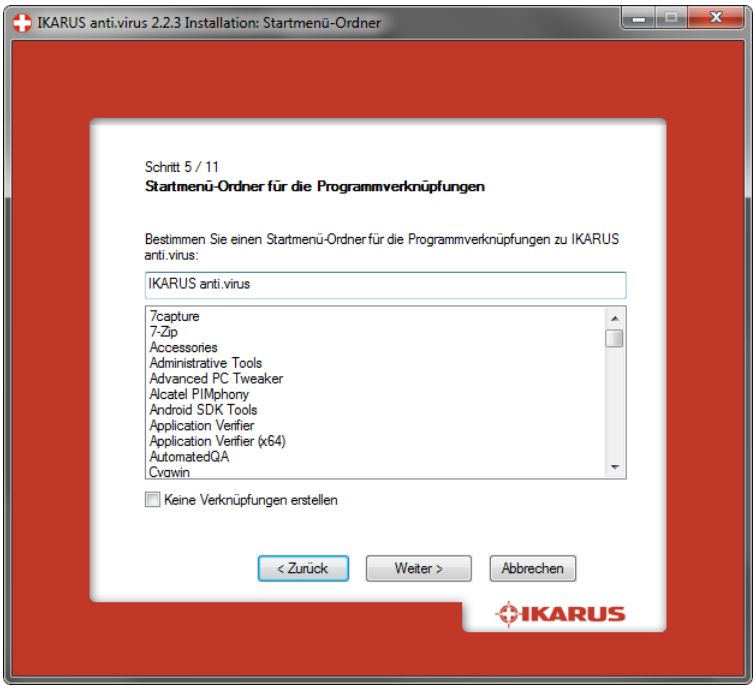
Achtung: Eine ältere Version von **IKARUS anti.virus** wird automatisch entfernt. Sie werden nach der Deinstallation vermutlich aufgefordert, den Rechner neu zu starten. Bitte führen Sie diesen Neustart durch, die Installation von **IKARUS anti.virus** startet danach automatisch.



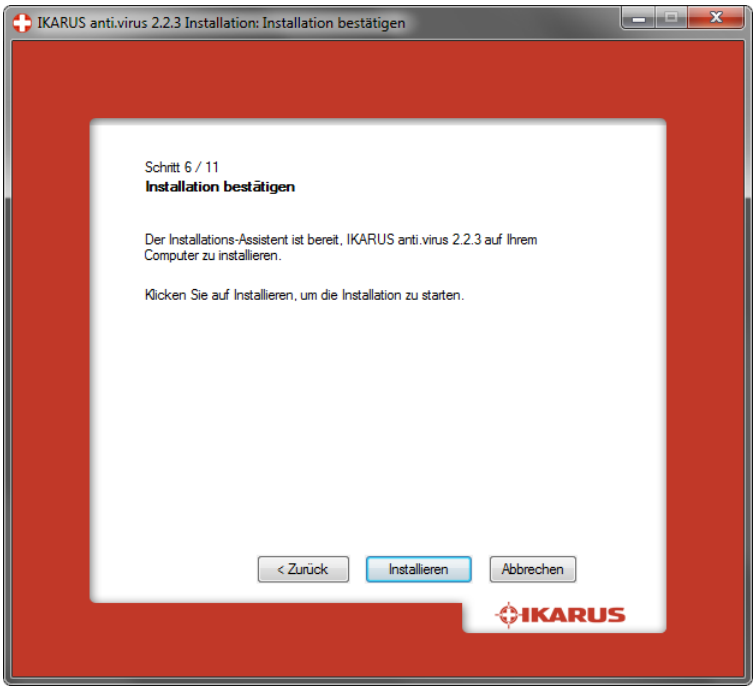
Schritt 4: Wählen Sie das Zielverzeichnis für die Installation von **IKARUS anti.virus** aus. Wir empfehlen, den vorgeschlagenen Standardordner beizubehalten.


IKARUS anti.virus 2.2.3 Installation: Zielverzeichnis auswählen
Schritt 4 / 11
Installationsverzeichnis für IKARUS anti.virus
IKARUS anti.virus 2.2.3 wird in das folgende Verzeichnis installiert.
Um in das unten angegebene Verzeichnis zu installieren, klicken Sie auf [Weiter]. Um in ein anderes Verzeichnis zu installieren, klicken Sie auf [Durchsuchen] und wählen Sie ein anderes Verzeichnis aus. Klicken Sie auf [Weiter], um fortzufahren.
C:\Program Files (x86)\IKARUS\anti.virus
Durchsuchen...
Verfügbarer Speicher: 679.6GB
Benötigter Speicher: 50.8MB
< Zurück
Weiter >
Abbrechen
IKARUS

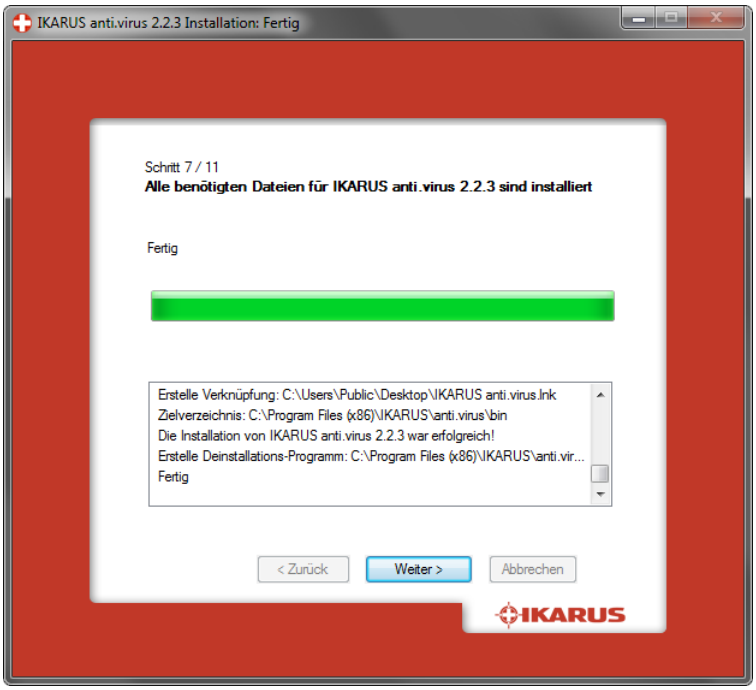
Schritt 5: Hier können Sie entscheiden, ob **IKARUS anti.virus** über das Startmenü aufgerufen werden kann. Wir empfehlen, die Voreinstellungen beizubehalten.



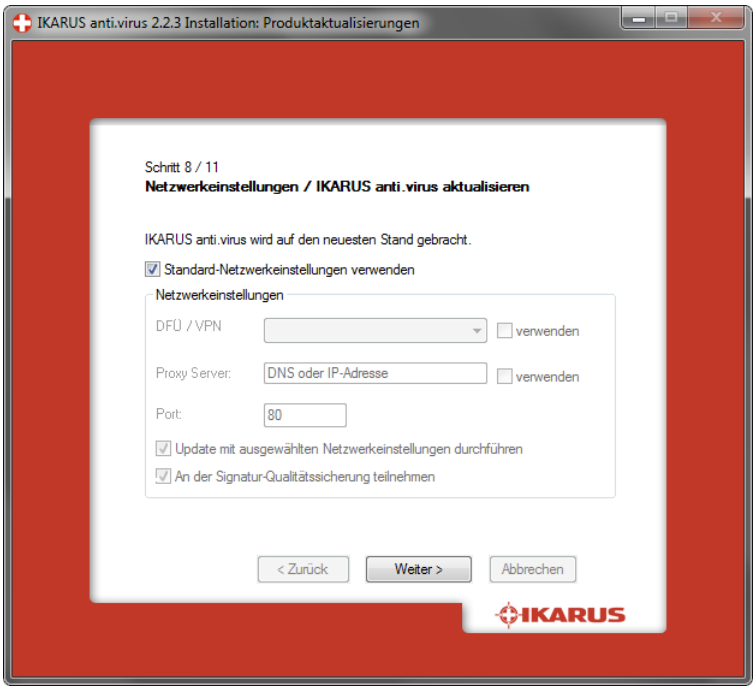
Schritt 6: Um die Installation zu starten, benötigt Ihr PC das Microsoft-Programm NET Framework. Haben Sie NET Framework von Microsoft noch nicht installiert, wird dies automatisch nachgeholt.


IKARUS anti.virus 2.2.3 Installation: Installation bestätigen
Schritt 6 / 11
Installation bestätigen
Der Installations-Assistent ist bereit, IKARUS anti.virus 2.2.3 auf Ihrem Computer zu installieren.
Klicken Sie auf Installieren, um die Installation zu starten.
< Zurück
Installieren
Abbrechen
IKARUS

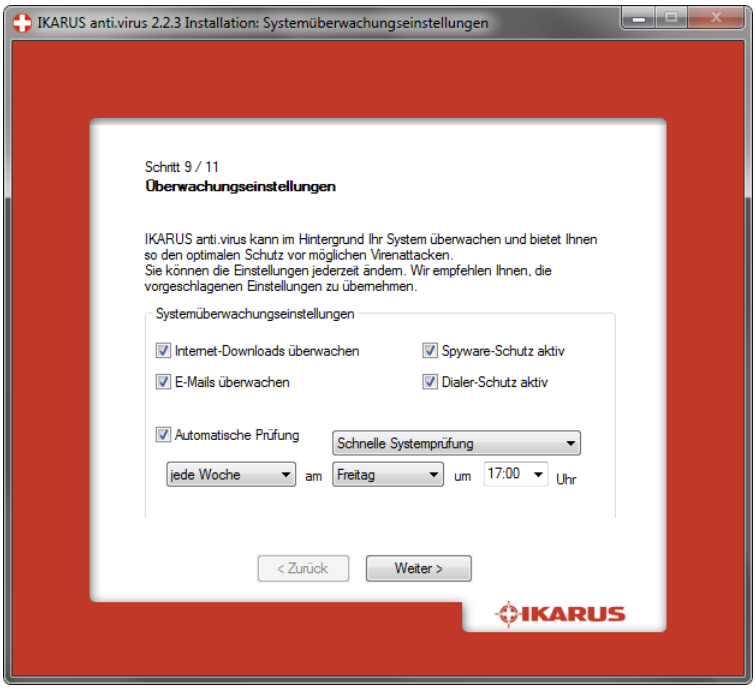
Schritt 7: Hier sehen Sie den Fortschritt der Installation. Klicken Sie nach Abschluss der Installation auf ”Weiter”.



Schritt 8: Jetzt werden die Internet-Einstellungen Ihres PCs überprüft. Diese Einstellungen sind notwendig, um **IKARUS anti.virus** regelmäßig zu aktualisieren. Wir empfehlen Ihnen, diese Voreinstellungen beizubehalten.



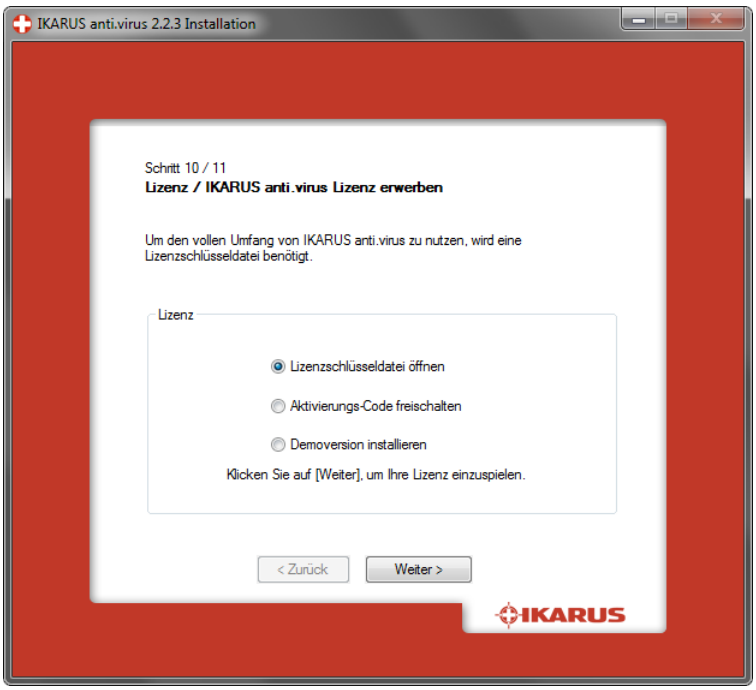
Schritt 9: Hier legen Sie die Überwachungseinstellungen fest. Wir empfehlen, diese Voreinstellungen beizubehalten. Sie können diese Einstellungen auch zu einem späteren Zeitpunkt direkt im Programm ändern.



Wählen Sie für die automatische Prüfung einen Zeitraum, zu dem Ihr PC üblicherweise eingeschaltet ist. Generell untersucht die voreingestellte ”Schnelle Systemprüfung” die wichtigsten Teile Ihres PCs. Wir empfehlen jedoch von Zeit zu Zeit auch eine Prüfung des gesamten PCs durchzuführen.

Mit der Auswahl ”Systempartitionen” wird der Datenträger überprüft, auf dem Sie Ihr Betriebssystem installiert haben. Meistens ist dies das Laufwerk C:\.

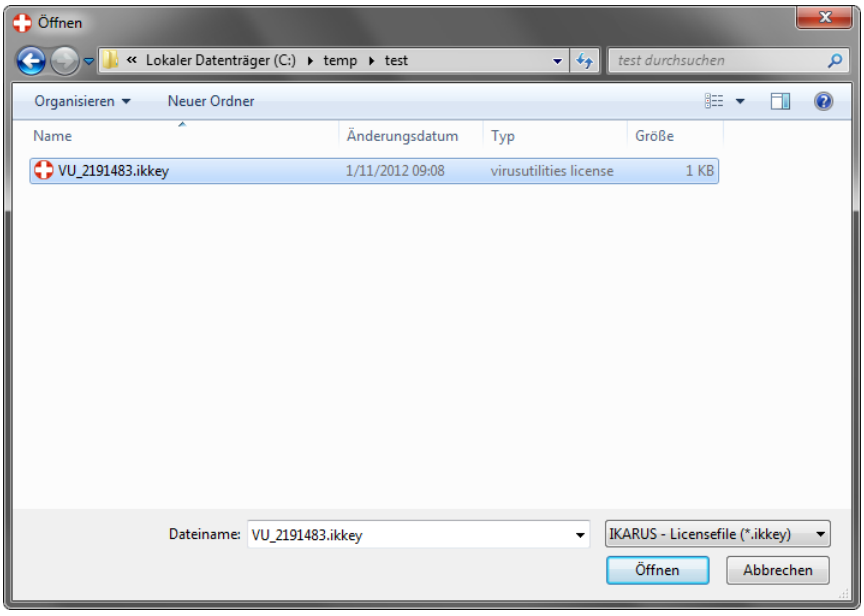
Schritt 10: Wählen Sie die Art der Registrierung von **IKARUS anti.virus**.


IKARUS anti.virus 2.2.3 Installation
Schritt 10 / 11
Lizenz / IKARUS anti.virus Lizenz erwerben
Um den vollen Umfang von IKARUS anti.virus zu nutzen, wird eine Lizenzschlüsseldatei benötigt.
Lizenz
Lizenzschlüsseldatei öffnen
Aktivierungs-Code freischalten
Demoversion installieren
Klicken Sie auf [Weiter], um Ihre Lizenz einzuspielen.
< Zurück
Weiter >
IKARUS

Es gibt folgende Möglichkeiten, **IKARUS anti.virus** zu registrieren:

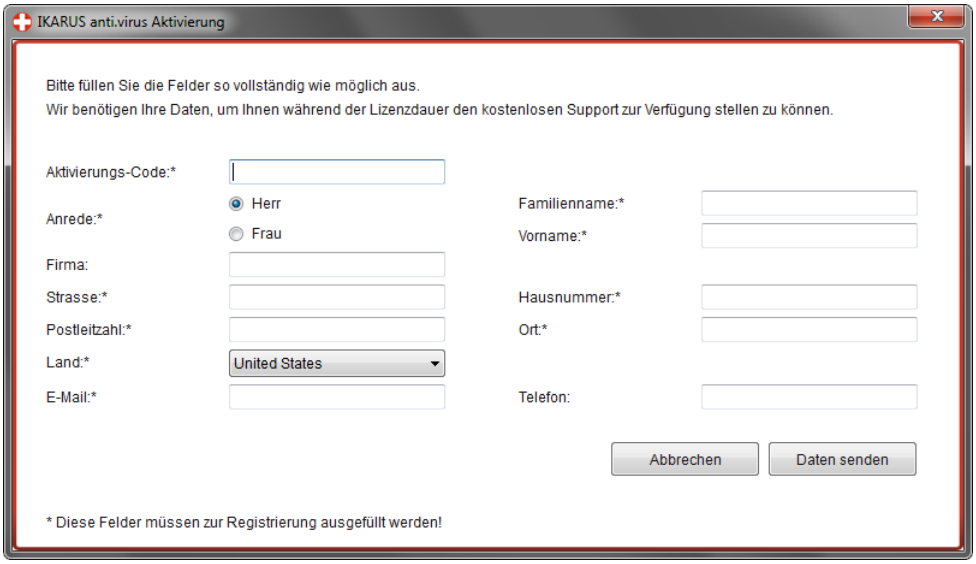
Lizenzschlüsseldatei öffnen

Definieren Sie hier Ihren persönlichen Lizenzschlüssel, den Sie von **IKARUS** erhalten haben.



Aktivierungs-Code freischalten

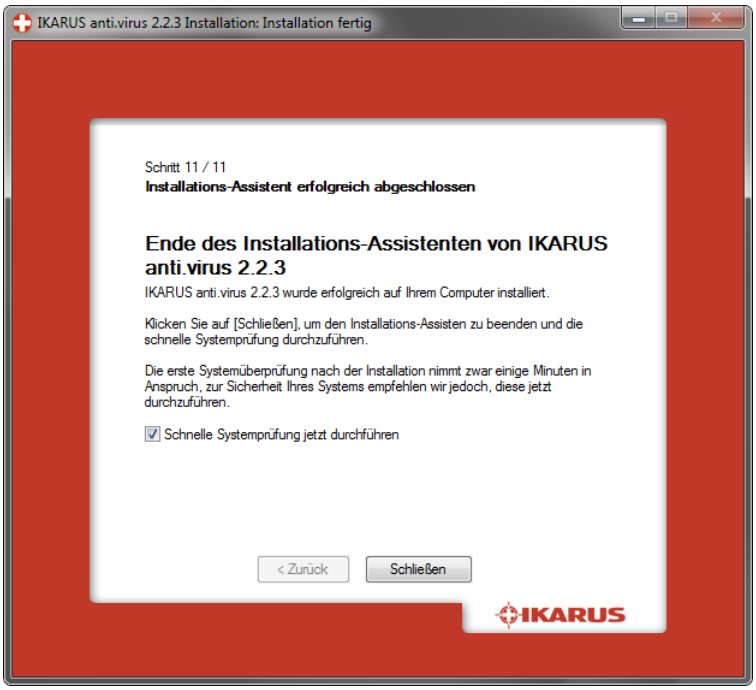
Mit Hilfe des Aktivierungscodes und der dazugehörigen Registrierung erhalten Sie von **IKARUS** einen Lizenzschlüssel, der vollautomatisch in die Software integriert wird. Die Lizenzdauer beginnt mit dem Datum der Registrierung.



Demoversion installieren

Testen Sie **IKARUS anti.virus** 30 Tage lang unverbindlich und kostenlos. Einen Demo-Lizenzschlüssel erhalten Sie auf unserer Homepage http://www.ikarus.at.

Schritt 11: Nun ist die Installation von **IKARUS anti.virus** abgeschlossen. Wir empfehlen, die schnelle Systemprüfung auf alle Fälle durchzuführen!


IKARUS anti.virus 2.2.3 Installation: Installation fertig
Schritt 11 / 11
Installations-Assistent erfolgreich abgeschlossen
Ende des Installations-Assistenten von IKARUS anti.virus 2.2.3
IKARUS anti.virus 2.2.3 wurde erfolgreich auf Ihrem Computer installiert.
Klicken Sie auf [Schließen], um den Installations-Assisten zu beenden und die schnelle Systemprüfung durchzuführen.
Die erste Systemüberprüfung nach der Installation nimmt zwar einige Minuten in Anspruch, zur Sicherheit Ihres Systems empfehlen wir jedoch, diese jetzt durchzuführen.
Schnelle Systemprüfung jetzt durchführen
< Zurück
Schließen
IKARUS

2.3 Installation von der Kommandozeile

Mit der Installation von der Kommandozeile aus bestehen weitere Möglichkeiten zur Konfiguration von **IKARUS anti.virus**.

Wichtig: Diese Form der Installation ist nur für fortgeschrittene Benutzer und Systemadministratoren geeignet.

Hier finden Sie eine Übersicht über alle verfügbaren Optionen:

Option	Parameter **(Standardwerte)**	Funktion
`/S`	-	use silent install
`-acceptlicenseagreement`	-	has to be accepted
`-oldikarus`	uninstall, **abort**	uninstalls old version
`-outlook`	kill, wait	how to behave if outlook is running
`-instdir`	path	program installation dir (automatically ends with ”anti.virus”)
`-startmenue`	path, no	make startmenue entry (automatically ends with ”anti.virus”). Use relative path.
`-dotnet`	path, download from MS	exe of .NET used if not installed
`-msi`	path, download from MS	exe of Microsoft Installer used if not installed
`-config`	path	Configfile to be used. Therefore parameters will be ignored
`-vdb`	path, no	path to an existing t3sigs.vdb
`-noupdatenow`	-	(for setup) default: make update
`-license`	path, demolicense	to get license from given path
`-nosystemscan`	-	no system scan starts after setup
`-allowreboot`	-	default: reboot no
`-log`	path, -	Folder for Setup-Logfile. Default: no Logfile is written at all If Option is given without argument,

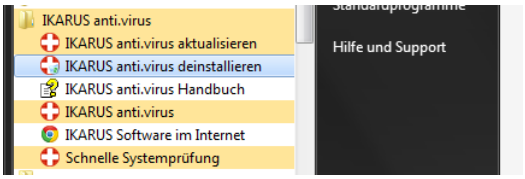
		a log file will be generated in the current directory.
`-useproxy`	yes (used if registry key is set),no	Use proxy server if set in Registry
`-proxy`	server:port	Specify proxy server
`-usedialin`	yes, no	use a dialin connection
`-dialin`		dialin connection name
`-update`	yes,no	enable updats
`-ismx`	host:port	update from ismx server will be set in guardx.conf
`-disablekickoff`	-	disables popup menu
`-allowinternetupdate`	-	allows ismx-managed anti.virus to update from internet
`-wsystem`	yes, no	enable system protection
`-wemail`	yes, no	enable mail protection
`-wdownloads`	yes, no	enable internet download protection
`-wspyware`	yes, no	enable spyware protection
`-wdialer`	yes, no	enable dialer protection
`-autoscan`	yes, no	enable automatic scheduled scan
`-scantype`	quick, standard, full	scantype for automatic scheduled scan
`-daily`	-	interval for automatic scan
`-weekly`	0-6, weekly 5 (Friday)	interval for automatic scan (0 = Sunday)
`-monthly`	1-31	interval for automatic scan
`-scanhour`	xx:xx, 17:00	time for automatic scan

Beispiel:

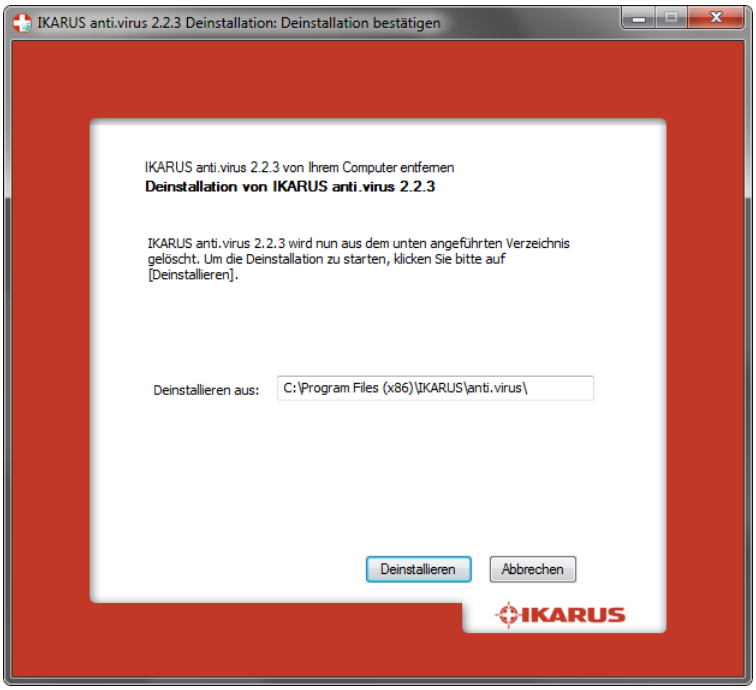
```
C:\temp> "Setup IKARUS anti.virus 2.2.3.exe" /S -acceptlicenseagreement -oldikarus uninstall
          -outlook kill -noupdate -instdir C:\Programme\Ikarus\antivirus -nosystemscan
```

2.4 Deinstallation von IKARUS anti.virus

Um **IKARUS anti.virus** zu deinstallieren, öffnen Sie den Programm-Ordner im Start-Menü.

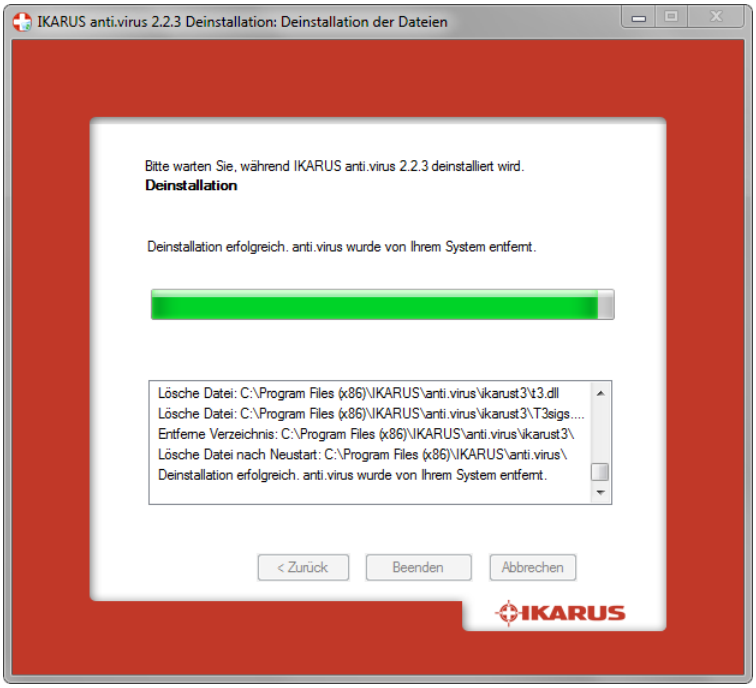


Nachdem Sie auf ”IKARUS anti.virus deinstallieren” geklickt haben, öffnet sich folgendes Fenster:

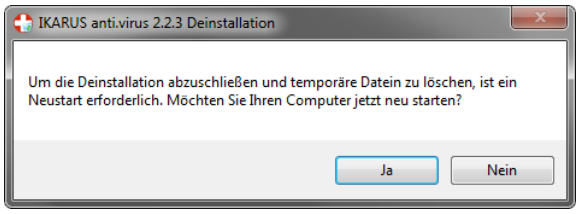

IKARUS anti.virus 2.2.3 Deinstallation: Deinstallation bestätigen
IKARUS anti.virus 2.2.3 von Ihrem Computer entfernen
Deinstallation von IKARUS anti.virus 2.2.3
IKARUS anti.virus 2.2.3 wird nun aus dem unten angeführten Verzeichnis gelöscht. Um die Deinstallation zu starten, klicken Sie bitte auf [Deinstallieren].
Deinstallieren aus:
C:\Program Files (x86)\IKARUS\anti.virus\
Deinstallieren
Abbrechen
IKARUS

Klicken Sie auf ”Deinstallieren”, um fortzufahren. Der Fortschritt der Deinstallation wird Ihnen angezeigt.

Wenn die Deinstallation abgeschlossen ist, erscheint ein entsprechender Hinweis im Fenster.


IKARUS anti.virus 2.2.3 Deinstallation: Deinstallation der Dateien
Bitte warten Sie, während IKARUS anti.virus 2.2.3 deinstalliert wird.
Deinstallation
Deinstallation erfolgreich. anti.virus wurde von Ihrem System entfernt.
Lösche Datei: C:\Program Files (x86)\IKARUS\anti.virus\ikarust3\t3.dll
Lösche Datei: C:\Program Files (x86)\IKARUS\anti.virus\ikarust3\T3sigs....
Entferne Verzeichnis: C:\Program Files (x86)\IKARUS\anti.virus\ikarust3\
Lösche Datei nach Neustart: C:\Program Files (x86)\IKARUS\anti.virus\
Deinstallation erfolgreich. anti.virus wurde von Ihrem System entfernt.
< Zurück
Beenden
Abbrechen
IKARUS

Gleichzeitig werden Sie gefragt, ob Sie Ihren Computer neu starten möchten.


IKARUS anti.virus 2.2.3 Deinstallation
Um die Deinstallation abzuschließen und temporäre Datein zu löschen, ist ein Neustart erforderlich. Möchten Sie Ihren Computer jetzt neu starten?
Ja
Nein

Es wird empfohlen, diesen Neustart sobald wie möglich durchzuführen. Dies ist vor allem unbedingt notwendig, wenn Sie planen, **IKARUS anti.virus** erneut zu installieren.

3 Funktionen von IKARUS anti.virus

IKARUS anti.virus bietet Ihnen:

- Schutz vor Virenbefall beim Surfen im Internet
- Schutz beim Mailen mit MS Outlook und Outlook Express
- Schutz vor unerwünschten Installationen von Dialern
- Schutz vor unerwünschter Ad- und Spyware
- Schutz vor Virenbefall durch mobile Datenträger, wie USB-Sticks
- Überprüfung der installierten Datenträger auf Virenbefall
- Automatische Aktualisierung der Programme und der Virendatenbank

3.1 Symbole und Anzeigen

Machen Sie sich nun mit den Symbolen von **IKARUS anti.virus** vertraut. Das Standardsymbol finden Sie rechts unten in der Taskleiste Ihres PCs.

Durch Doppelklicken auf das Symbol öffnet sich automatisch die Konfigurationsmaske von **IKARUS anti.virus**. Wenn Sie mit dem Mauszeiger über das Symbol fahren, erscheint für einige Sekunden das folgende Fenster:

Sie können **IKARUS anti.virus** auch über dieses Fenster öffnen. Klicken Sie dazu in das gewünschte Feld (Scan, Update oder Guard). Sie sehen hier auf einen Blick, ob **IKARUS anti.virus** einwandfrei läuft, wann es zuletzt aktualisiert wurde, wann die letzte Prüfung durchgeführt wurde und ob alle Komponenten des Virenschutzes aktiviert sind.

Die Darstellung des Symbols in der Taskleiste kann sich verändern und hat jeweils eine andere Bedeutungen:

Das weiß-rote Kreuz zeigt Ihnen, dass alles in Ordnung und der Virenschutz optimal eingestellt und aktualisiert ist. **IKARUS anti.virus** ist aktiv und überwachet Ihren PC.

Dieses Symbol zeigt an, dass einer der Bereiche Scan, Update oder Guard nicht den hohen Sicherheitsrichtlinien von **IKARUS anti.virus** entspricht. Wenn Sie das Informationsfenster öffnen, sehen Sie, welcher Bereich von der Warnung betroffen ist.

In diesem Beispiel wurde ein Teil des Guards, d.h. ein Teil der Überprüfung, deaktiviert.

Ein größer und kleiner werdendes Symbol (ähnlich einem Herzschlag) zeigt, dass **IKARUS anti.virus** gerade aktualisiert wird.

Ein sich drehendes Symbol wiederum ist das Zeichen für einen aktuell laufenden Scan.

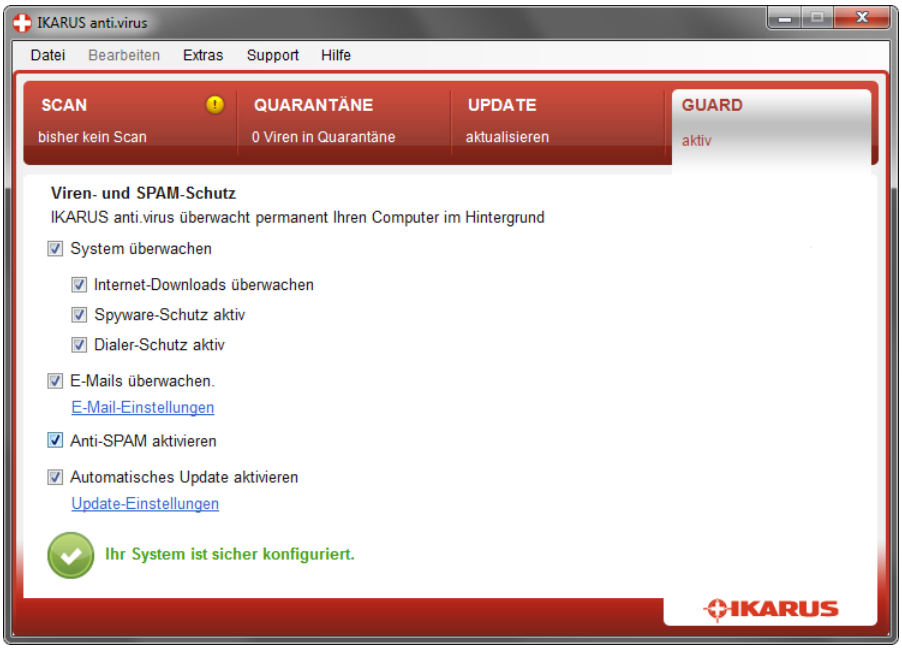
Sieht Ihr **IKARUS anti.virus** Symbol in der Taskleiste so aus, wissen Sie, dass ein Virus gefunden wurde.

Was dann zu tun ist, erfahren Sie unter Was tun bei Virenfund - die Quarantäne.

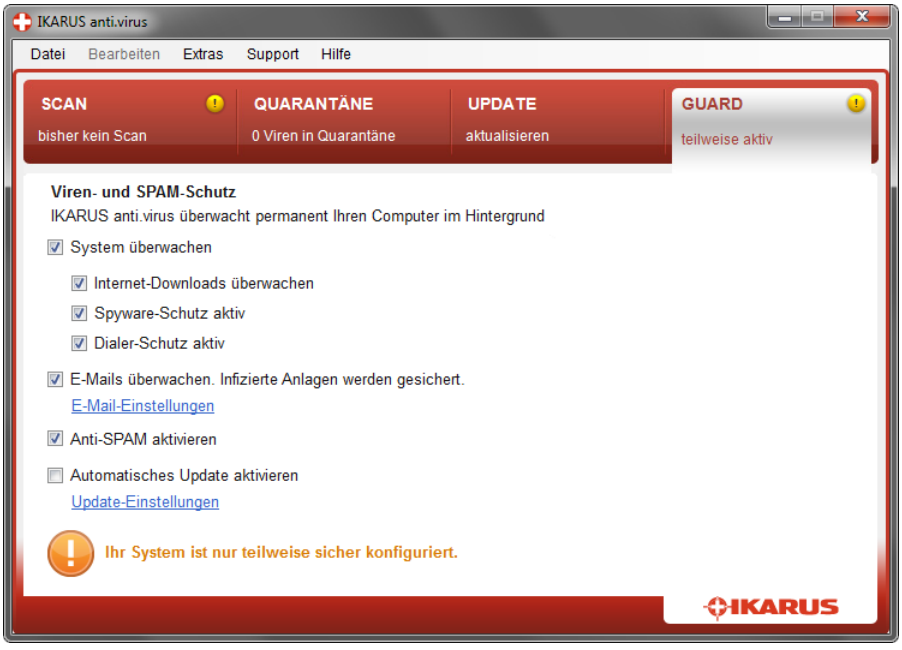
4 Der Guard - Ihr Sicherheitswächter

Der Guard ist das Wächter-Programm von **IKARUS anti.virus**. Eine Aktivierung aller Checkboxen bietet Ihnen den größtmöglichen Schutz vor Schadprogrammen. Nach Bedarf können Sie die Virenschutzeinstellungen ”lockern” und eine oder mehrere der Checkboxen deaktivieren.

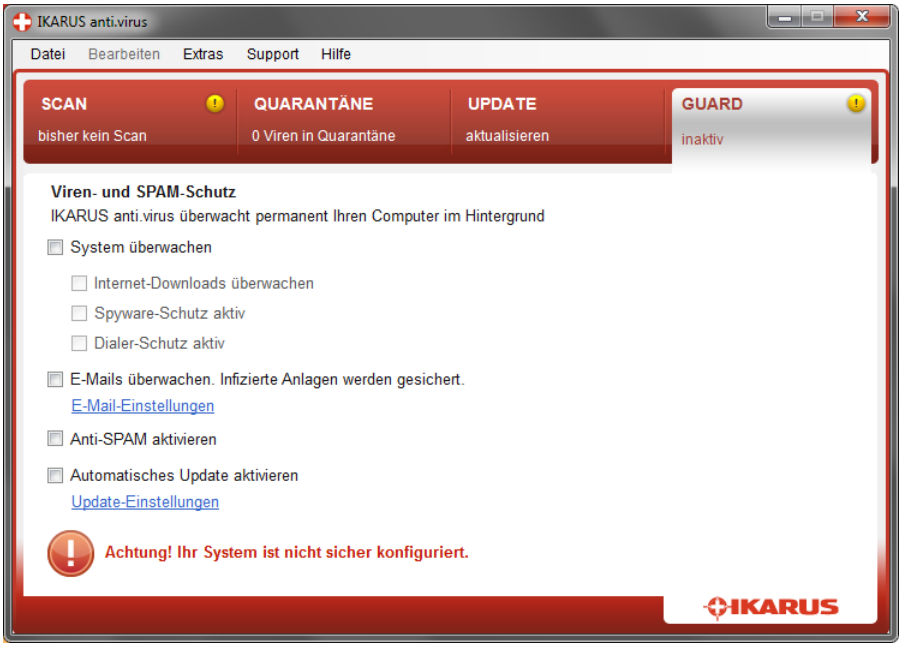
Achtung: Nur wenn alle Optionen ausgewählt und aktiviert sind, bieten Ihnen **IKARUS anti.virus** den höchstmöglichen Virenschutz!



Wenn eine oder mehrere Sicherheitseinstellungen inaktiv sind, erkennen Sie das am gelben Symbol und dem Text ”Ihr System ist nur teilweise sicher konfiguriert”.



Sollten Sie ein rotes Symbol erkennen können, so ist der IKARUS Guard außer Kraft und die Meldung ”Achtung! Ihr System ist nur teilweise sicher konfiguriert” erscheint.



Wurden ein oder mehrere Bereiche von der Prüfung ausgenommen, so sehen Sie dies auch am veränderten **IKARUS anti.virus**-Symbol in der Taskleiste. **IKARUS anti.virus** bietet Ihnen dann nicht mehr den optimalen Schutz!

5 Das Update von IKARUS anti.virus

Nur ein aktueller Virenschutz ist auch ein zuverlässiger Schutz vor Viren, Würmern, Spyware und Trojanern!

IKARUS anti.virus verfügt über eine automatische Aktualisierung. Das Programm überprüfet regelmäßig (alle 20 Minuten), ob ein neues Update zur Verfügung steht.

Neue Updates werden automatisch installiert. Bei Bedarf wird dazu eine Internet-Verbindung aufgebaut.

Haben Sie Ihren PC längere Zeit nicht in Betrieb gehabt, so aktualisieret sich **IKARUS anti.virus** automatisch nach dem Starten des PCs.

Das Update von **IKARUS anti.virus** unterscheidet zwischen dem Viren-Datenbank-Update und jenem von **IKARUS anti.virus** selbst.

Updates der Virendatenbank (VDB) garantieren Ihnen, dass auch neue Schadensprogramme erkannt werden. Bei den Updates von **IKARUS anti.virus** handelt es sich um Programmupdates, um Ihnen z.B. Programmneuheiten oder neue Features zugänglich zu machen.

Über den Button ”Jetzt Updaten” können Sie jederzeit eine Aktualisierung durchführen.

Ist **IKARUS anti.virus** bereits auf dem neuesten Stand, erhalten Sie die Mitteilung ”Alles am neuesten Stand”.

6 Der Scan - die Virenprüfung von IKARUS anti.virus

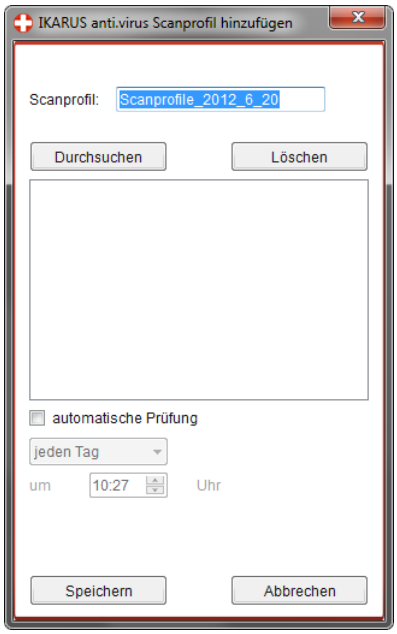
Der Scanvorgang von **IKARUS anti.virus** kann sowohl automatisch als auch händisch angestoßen werden.

Sie können beliebig viele Scans anlegen und verwalten.

Voreingestellte Scans sind:

- **Schnelle Systemprüfung:** Mit dieser Auswahl prüfen Sie unter anderem das Windows Installations-Verzeichnis. Die meisten Computerschädlinge befinden sich in diesem Verzeichnis und können so zuverlässig und rasch erkannt werden.
- **Systempartition: IKARUS anti.virus** scannt mit dieser Auswahl jenes Laufwerk, auf dem Ihr Betriebssystem installiert ist. Sämtliche Archive, Verzeichnisse, Ordner und Dateien, die auf diesem Laufwerk liegen, werden von **IKARUS anti.virus** überprüft.
- **Gesamter Computer:** Alle Laufwerke des PCs werden von **IKARUS anti.virus** gescannt.
- **Wechseldatenträger** Hier werden alle externen Datenträger wie beispielsweise USB-Sticks oder CD-ROM überprüft.

Individuelle Scans werden durch den Button ”Scanprofil hinzufügen” editiert.

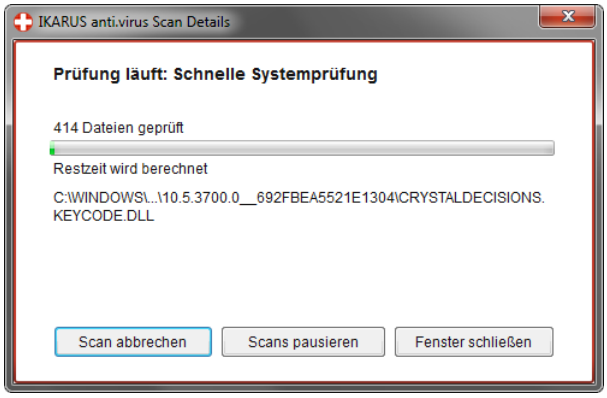


Sie können dem Scanprofil einen beliebigen Namen geben. Mit dem Button ”Durchsuchen” wählen Sie die zu scannenden Ordner, Dateien etc. aus.

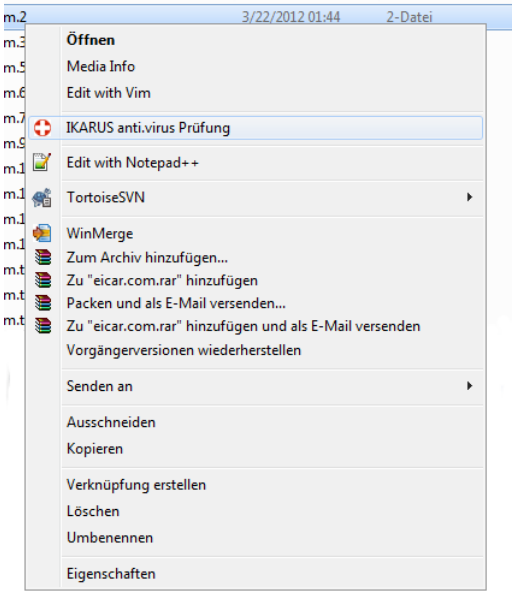
Außerdem können Sie festlegen, ob Sie eine automatische Prüfung einstellen wollen.

Die automatische Prüfung kann zu einem beliebigen Zeitpunkt festgelegt werden (z.B.: jeden Freitag um 12 Uhr) und scannt dann die von Ihnen definierten Bereiche.

Um einen Scan manuell zu aktivieren, klicken Sie einfach auf ”Jetzt Scannen”.



Eine weitere Möglichkeit einen Scan zu starten, bietet der Windows Explorer: Wählen Sie ein Laufwerk, eine Datei oder einen Ordner aus und starten Sie über die rechte Maustaste die **IKARUS anti.virus** Prüfung.



Einen gestarteten Scan können Sie jederzeit beenden bzw. abbrechen.

Am Fortschrittsbalken und an der angezeigten Restzeit können Sie den Verlauf des Scan-Vorgangs beobachten.

Ist der Scan beendet und wurde kein Virus gefunden, kommen Sie mit Klick auf den Button ”Fenster schließen” zum Hauptmenü zurück.

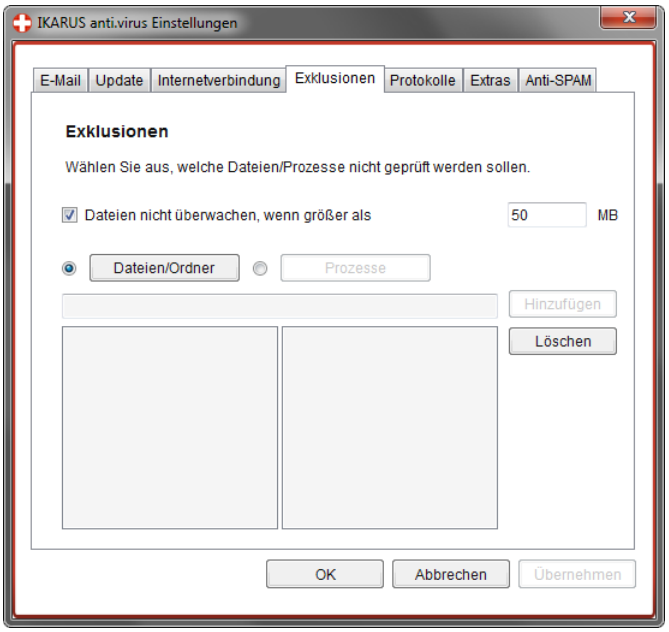
Was bei einem Virenfund zu tun ist, lesen Sie unter Was tun bei Virenfund - die Quarantäne.

6.1 Die Scan-Einstellungen

Über den Menüpunkt ”Einstellungen” gelangen Sie über den Reiter ”Exklusionen” zu den Einstellungen für den Scan.

Hier können Sie z.B. festlegen, welche Dateien und Prozesse von dem Scanvorgang durch **IKARUS anti.virus** ausgenommen sind.

Eine wetere Möglichkeit zur Exclusion ist die Größe einer Datei betreffen.


IKARUS anti.virus Einstellungen
E-Mail
Update
Internetverbindung
Exklusionen
Protokolle
Extras
Anti-SPAM
Exklusionen
Wählen Sie aus, welche Dateien/Prozesse nicht geprüft werden sollen.
Dateien nicht überwachen, wenn größer als
50
MB
Dateien/Ordner
Prozesse
Hinzufügen
Löschen
OK
Abbrechen
Übernehmen

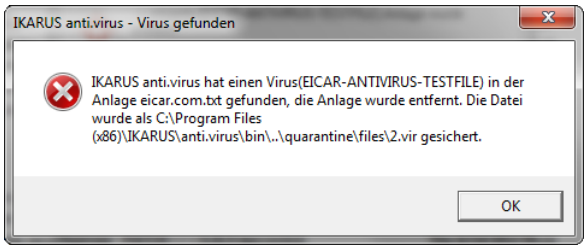
7 Was tun bei Virenfund - die Quarantäne

Lesen in diesem Kapitel, wo Sie alle gefundenen Viren sehen und bearbeiten können und welche Möglichkeiten Sie in der Quarantäne von **IKARUS anti.virus** haben, um eine infizierte Datei sicher von Ihrem System zu entfernen.

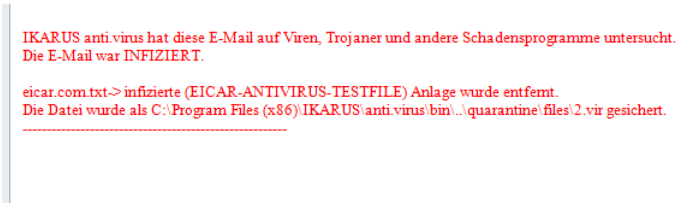
7.1 Anzeigen eines Virenfundes

Einen Virenfund zeigt Ihnen **IKARUS anti.virus** mit folgenden Meldungen an:

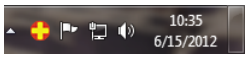
- Beim Empfang einer infizierten E-Mail erkennt **IKARUS anti.virus** das Schadprogramm. Es öffnet sich ein Fenster, in dem **IKARUS anti.virus** Sie darüber informiert, dass ein Virus gefunden und dieser in das Quarantäneverzeichnis verschoben wurde.


IKARUS anti.virus - Virus gefunden
IKARUS anti.virus hat einen Virus(EICAR-ANTIVIRUS-TESTFILE) in der Anlage eicar.com.txt gefunden, die Anlage wurde entfernt. Die Datei wurde als C:\Program Files (x86)\IKARUS\anti.virus\bin\..\quarantine\files\2.vir gesichert.
OK

- In der infizierten E-Mail selbst finden Sie bei einem Virenfund einen Text mit diesem Inhalt:


IKARUS anti.virus hat diese E-Mail auf Viren, Trojaner und andere Schadensprogramme untersucht.
Die E-Mail war INFIZIERT.
eicar.com.txt-> infizierte (EICAR-ANTIVIRUS-TESTFILE) Anlage wurde entfernt.
Die Datei wurde als C:\Program Files (x86)\IKARUS\anti.virus\bin\..\quarantine\files\2.vir gesichert.

- Auch das gelbe Icon von **IKARUS anti.virus** in der Taskleiste zeigt einen Virenfund an:

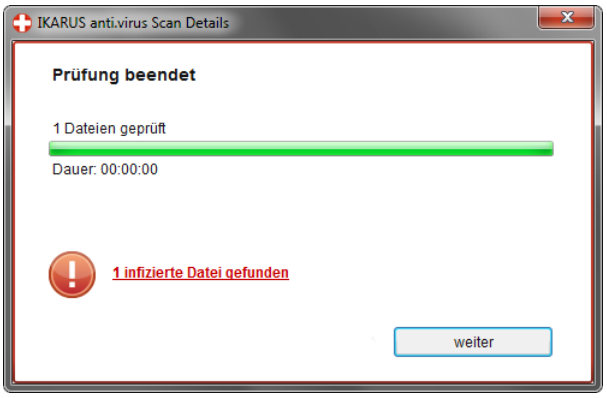


- Im Ansichtsfenster von **IKARUS anti.virus** wird der Virenfund mit rotem Balken und Warnhinweis im Scan-Fenster angezeigt.

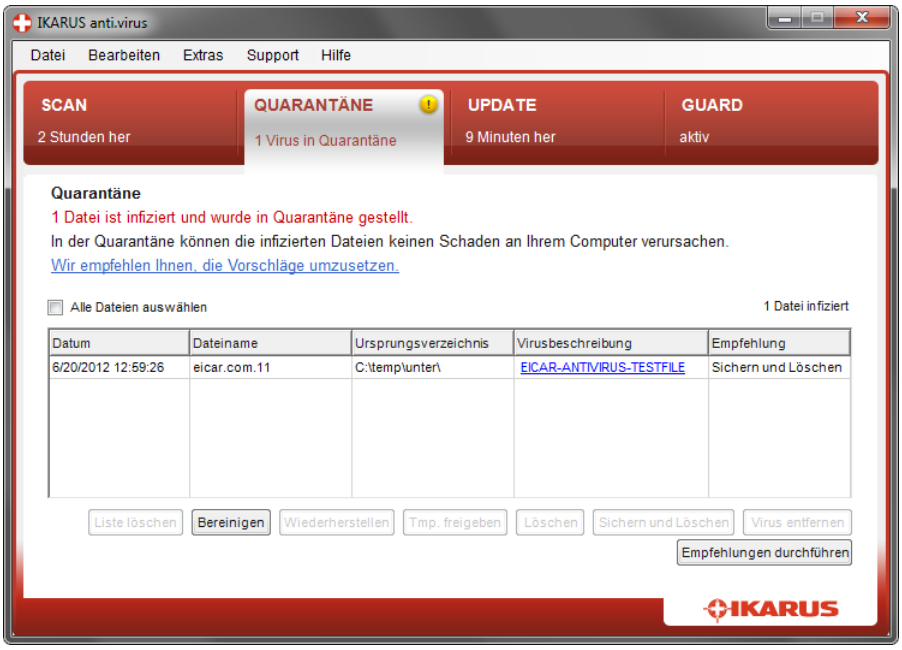
7.2 Virenfund beim Scanvorgang

Wenn Sie einen automatischen oder einen individuellen Scan gestartet haben und dabei ein Virus gefunden wird, sieht dies wie folgt aus.

- In der Taskleite wird das gelbe Icon von **IKARUS anti.virus** angezeigt sowie ein Warnhinweis im Ansichtsfenster.
- Im Scanfenster erscheint während und nach der Virensuche die Meldung ”infizierte Datei” gefunden.



- Nach Beendigung des Scan-Vorgangs von **IKARUS anti.virus** öffnet sich automatisch das Quarantäne-Fenster.



7.3 Die Quarantäne

Ein von **IKARUS anti.virus** gefundenes Virus wird automatisch in die Quarantäne verschoben. Ist das Virus einmal in der Quarantäne ”gefangen”, besteht für Ihr System keine Gefahr mehr vor diesem Virus.

Sobald eine infizierte Datei in die Quarantäne verschoben wurde, wird der Zugriff darauf automatisch gesperrt. Sie kann daher ab diesem Zeitpunkt keine Schadensfunktionen auf Ihren PC mehr ausführen.

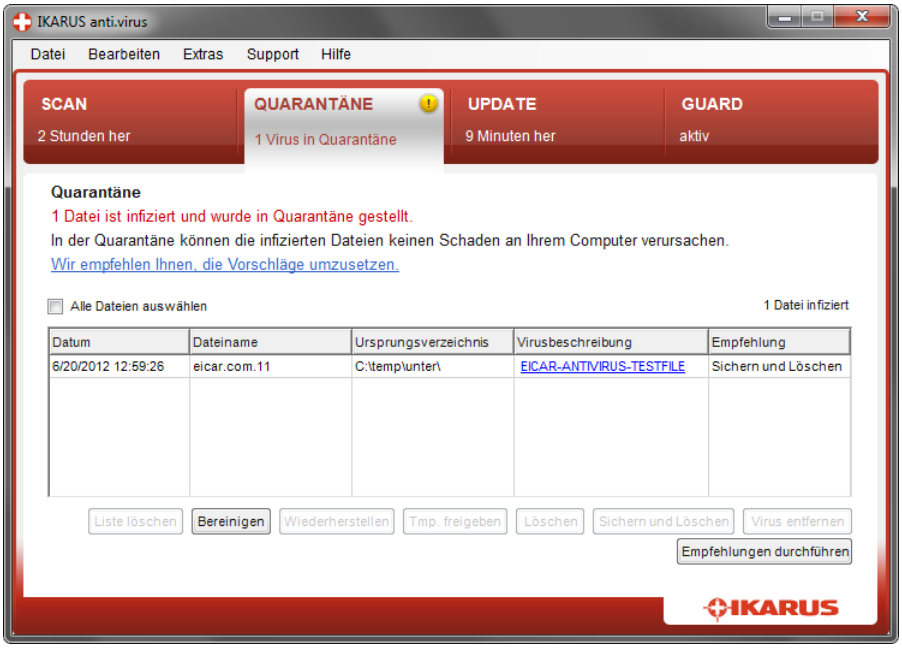
In der Quarantäne finden Sie alle notwendigen Informationen zu dem gefundenen Virus und über die Möglichkeiten der Entfernung.

Sie können alle Funktionen des Quarantäne-Fensters auch direkt über die Menüleiste und den Menüpunkt ”Bearbeiten” durchführen.

Die Quarantäne von **IKARUS anti.virus** bietet Ihnen verschiedene Möglichkeiten an, wie mit dem Virus bzw. der infizierten Datei umgegangen werden soll.

Überdies gibt Ihnen **IKARUS anti.virus** eine Empfehlung, welche Aktion im jeweiligen Fall am sinnvollsten erscheint.

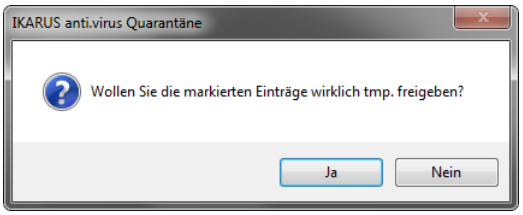
Mit Klick auf den Button ”Empfehlungen durchführen” werden die von **IKARUS anti.virus** vorgeschlagenen Aktionen ausgeführt.



Wollen Sie den Empfehlungen von **IKARUS anti.virus** nicht folgen, können Sie auch andere Aktionen wählen.

Mögliche Aktionen:

- **Bereinigen:** Alle infizierten Dateien werden in die Quarantäne verschoben.
- **Tmp.Freigeben:** Die als infiziert erkannte Datei wird temporär freigegeben. Das bedeutet, dass diese Datei bis zum Neustart des Services (d.h normalerweise bis zum Neustart des PCs) nicht mehr gemeldet wird. Dies ermöglicht Ihnen wieder den Zugriff auf diese Datei. Nach einem Neustart Ihres PCs finden Sie die Datei jedoch wieder in der Quarantäne. Nach Betätigen des Buttons werden Sie außerdem gefragt, ob Sie die infizierte Datei an **IKARUS** zur Analyse schicken möchten (anonym oder mit E-Mail Adresse zur Rückmeldung)



- **Löschen:** Die markierte Datei wird in die Quarantäne verschoben.

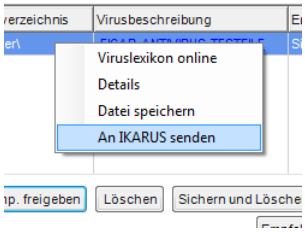
- **Sichern und löschen:** Die infizierte Datei wird in die Quarantäne verschoben. Gleichzeitig wird eine Sicherungskopie der Datei in Ihrem **IKARUS anti.virus**-Verzeichnis belassen. Der Eintrag in der Quarantäne wird danach hellgrau. Wenn gewünscht, können Sie die Datei durch Klick auf den Button ”Zurück verschieben” wiederherstellen.
- **Virus entfernen:** Wenn möglich, wird nur das Virus selbst aus der infizierten Datei entfernt. Die Datei selbst bleibt dabei bestehen und wird nicht gelöscht. Dateien, die im Grunde nur aus einem Virus bestehen, werden zur Gänze gelöscht.
- **Liste säubern:** Entfernt die Einträge aus der Quarantäneliste. Mehr als 7 Tage alte Einträge werden automatisch aus der Liste entfernt.

In der Quarantäneliste von **IKARUS anti.virus** können Sie jederzeit überprüfen, welche Viren bereits gefunden wurden, ob Viren gelöscht bzw. welche Aktionen durchgeführt wurden.

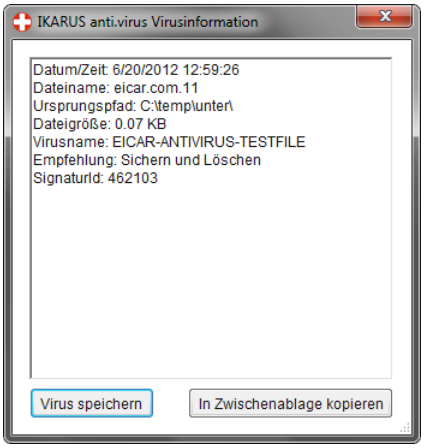
Schwarze Einträge bedeuten, dass ein Virus in Quarantäne ist und noch keine Aktionen gesetzt wurden. Entscheiden Sie, welche Aktion Sie durchführen wollen, oder führen Sie die Empfehlungen von **IKARUS anti.virus** durch.

Graue Einträge bedeuten, dass ein Virus gelöscht oder gesichert wurde. Sie können diese Einträge mit einem Klick auf ”Liste säubern” jederzeit entfernen.

Mit einem Klick der rechten Maustaste auf einen Vireneintrag in der Quarantäne können Sie ein Kontexmenü öffnen, in dem wiederum können Sie wiederum individuelle Aktionen festgelegt werden können.

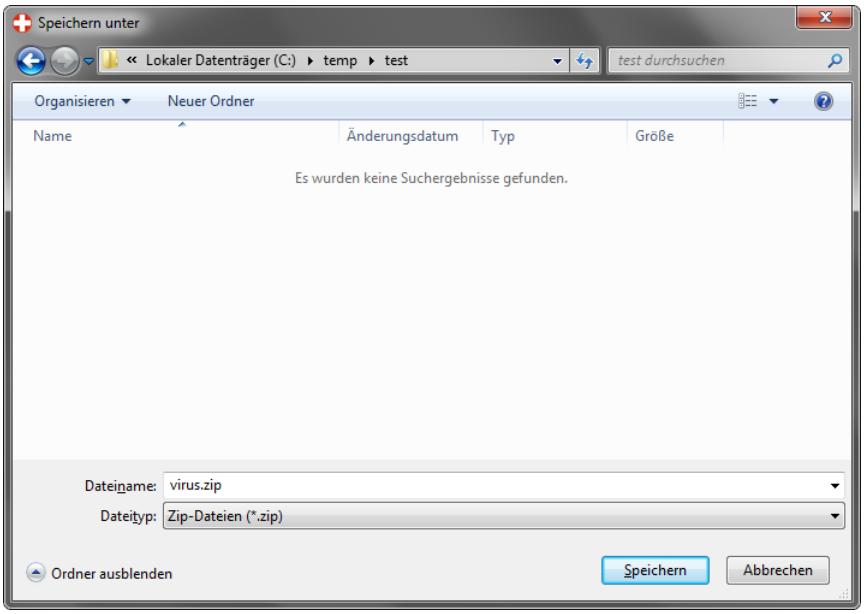


Wollen Sie mehr zu einem Virus erfahren, welches sich in Ihrer Quarantäne befindet, können Sie durch Doppelklick auf den Dateinamen bzw. das Ursprungsverzeichnis weitere Informationen erhalten.

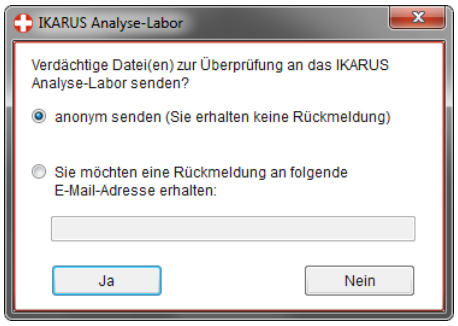


Mit einem Klick auf die jeweilige Virusbeschreibung im Quarantäne-Fenster verbinden Sie sich automatisch mit dem Virenlexikon auf der **IKARUS** Website und können so weitere Informationen zu dem Virus einholen.

Wenn Sie auf ”Datei speichern” klicken, wird automatisch eine Datei ”virus.zip” generiert, die Sie per E-Mail an **IKARUS** zur weiteren Analyse schicken können.



Um die infizierte Datei automatisch an **IKARUS** zu versenden, benützen Sie bitte die Funktion ”An IKARUS senden”.


IKARUS Analyse-Labor
Verdächtige Datei(en) zur Überprüfung an das IKARUS Analyse-Labor senden?
anonym senden (Sie erhalten keine Rückmeldung)
Sie möchten eine Rückmeldung an folgende E-Mail-Adresse erhalten:
Ja
Nein

Sie haben die Möglichkeit, dies entweder anonym zu tun oder eine E-Mail-Adresse anzugeben, um eine Rückmeldung zu erhalten.

8 Anti-SPAM

Das IKARUS Anti-SPAM-Modul ermöglicht das Filtern von E-Mails, die mittels Outlook, Outlook Express oder Windows Mail abgerufen werden. Um den SPAM-Schutz zu aktivieren klicken Sie bitte in den Virenschutz-Einstellungen von **IKARUS anti.virus** auf die Option ”Anti-SPAM”.

Beim nächsten **IKARUS anti.virus**-Update wird die Anti-SPAM Funktion aktiviert.

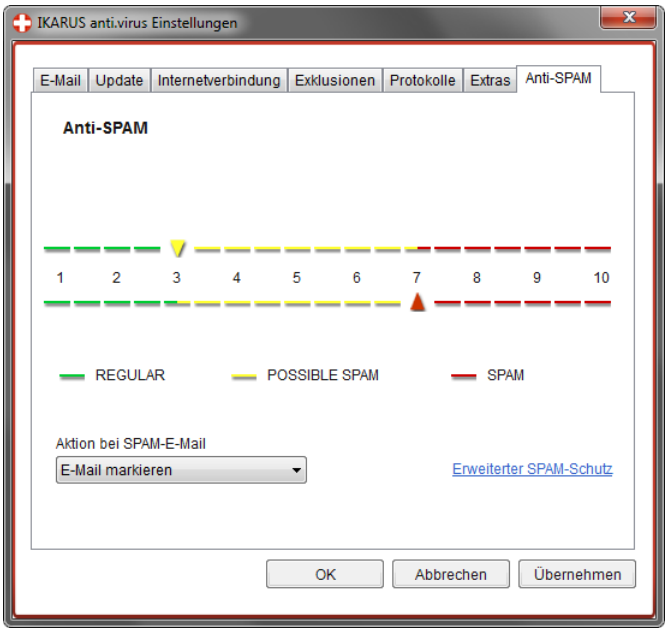
Mit den beiden Reglern (gelb bzw. rot) definiert man, ab welcher Bewertung eingehende E-Mails als ”SPAM” bzw. ”Possible SPAM” erkannt werden.

Zum Ändern der Standardeinstellung (3/7) klicken Sie in der jeweiligen Zeile (oben ”Possible SPAM”, unten ”SPAM”)auf die entsprechende farbige Markierung.

Als Aktion für E-Mails, die als SPAM bewertet wurden, lassen sich die Optionen ”Mail markieren” (hier wird der Betreff mit dem Wort ”SPAM” ergänzt) und ”Mail verschieben” (hier wird die E-Mail in den Junk-Ordner des Mailclients verschoben) auswählen.

E-Mails, die als ”Possible SPAM” erkannt wurden, werden im Betreff immer mit ”POSSIBLE SPAM” gekennzeichnet und bleiben im Posteingang des Mailclients.

Unter dem Punkt ”Erweiterter SPAM-Schutz” finden Sie die Möglichkeit weitere Einstellungen zu setzen, u.a. spezielle Filter zum Black- und Whitelisten von eingehenden E-Mails anhand von Sender, Empfänger, Inhalt oder Betreff.



9 Microsoft-SharePoint-Überwachung

Der folgende Abschnitt beschreibt die Verwendung von **IKARUS anti.virus** als Antiviren-Plugin für Microsoft SharePoint und wendet sich an fortgeschrittene Benutzer und Systemadministratoren.

Wenn SharePoint nicht auf Ihrem Computer installiert ist, ist dieser Abschnitt des Handbuches für Sie nicht von Bedeutung.

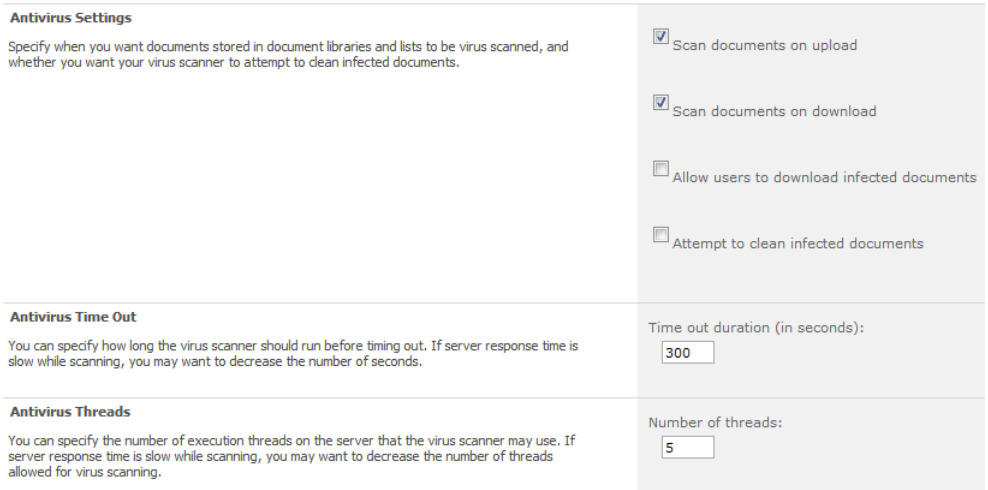
9.1 Leistungsumfang

IKARUS anti.virus 2.2 kann als Antiviren-Plugin für Microsoft SharePoint verwendet werden.

Der Schutz deckt zwei Bereiche ab:

- Dateien werden während des Uploads auf den Server gescannt, und der Upload wird unterbunden, wenn ein Virus gefunden wurde.
- Dateien werden während des Downloads vom Server gescannt, und der Download wird unterbunden, wenn ein Virus gefunden wurde.

In der Oberfläche von **IKARUS anti.virus** besteht nur die Möglichkeit, die SharePoint-Überwachung global zu aktivieren oder zu deaktivieren. Gesteuert wird das Plugin über die Administrationsoberfläche von Microsoft SharePoint. Zu beachten ist hier, dass die Option ”Attempt to clean infected documents” von **IKARUS anti.virus** nicht unterstützt wird und daher in jedem Fall wirkungslos bleibt.


Antivirus Settings
Specify when you want documents stored in document libraries and lists to be virus scanned, and whether you want your virus scanner to attempt to clean infected documents.
Scan documents on upload
Scan documents on download
Allow users to download infected documents
Attempt to clean infected documents
Antivirus Time Out
You can specify how long the virus scanner should run before timing out. If server response time is slow while scanning, you may want to decrease the number of seconds.
Time out duration (in seconds):
300
Antivirus Threads
You can specify the number of execution threads on the server that the virus scanner may use. If server response time is slow while scanning, you may want to decrease the number of threads allowed for virus scanning.
Number of threads:
5

Wichtig: Das **IKARUS anti.virus**-Plugin erfordert SharePoint Server Version 2007 oder höher und setzt ein 64-bit Betriebssystem voraus.

9.2 Installation

Führen Sie die Installation von **IKARUS anti.virus** durch, wie in Abschnitt 2 beschrieben. **IKARUS anti.virus** erkennt einen bereits installierten Microsoft SharePoint automatisch, aber Sie müssen nach erfolgter Installation dennoch den Microsoft IIS neu starten, um die Registrierung des Plugins abzuschließen. Ebenso müssen Sie den Microsoft IIS neu starten, um nach einer eventuellen Deinstallation von **IKARUS anti.virus** die Reregistrierung des Plugins abzuschließen.

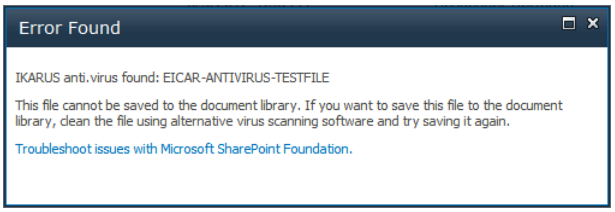
Beachten Sie außerdem, dass die Installation nur dann erfolgreich ist, wenn nicht bereits eine andere Antiviren-Software mit SharePoint-Unterstützung auf Ihrem Rechner installiert wurde.

Für die Client-Rechner, die sich mit Ihrem SharePoint-Server verbinden, ist keinerlei weitere Konfiguration nötig!

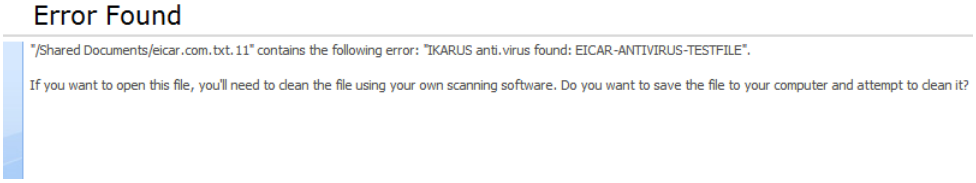
9.3 Arbeitsweise

In den Standardeinstellungen von SharePoint und **IKARUS anti.virus** wird jede hochgeladene oder heruntergeladene Datei einer Virenprüfung unterzogen. Wenn das Untersuchungsergebnis negativ ist, die Datei also nicht infiziert ist, bemerkt der Endbenutzer auf seinem Clientrechner nichts von diesem Vorgang und kann seine Arbeit ungestört fortsetzen.

Wird von **IKARUS anti.virus** jedoch ein Virus gefunden, wird die laufende Aktion unterbunden, und der Benutzer wird über ein Dialogfenster im Webbrowser informiert. Die folgende Abbildung zeigt das Dialogfenster, das dem SharePoint-Endbenutzer angezeigt wird, wenn **IKARUS anti.virus** in der hochzuladenden Datei einen Virus gefunden hat:

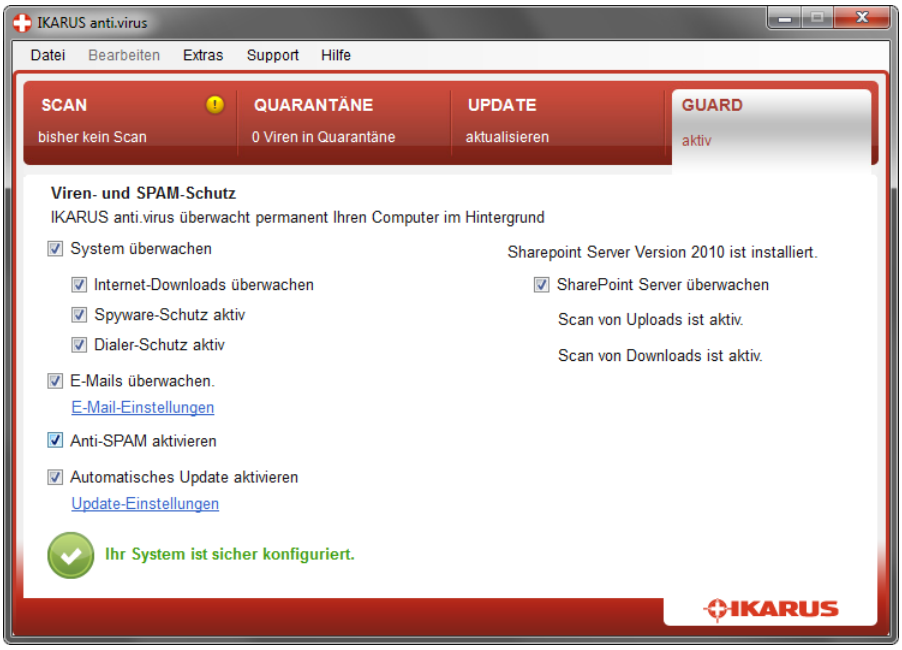

Error Found
IKARUS anti.virus found: EICAR-ANTIVIRUS-TESTFILE
This file cannot be saved to the document library. If you want to save this file to the document library, clean the file using alternative virus scanning software and try saving it again.
Troubleshoot issues with Microsoft SharePoint Foundation.

Hier hingegen das Dialogfenster, das beim Download einer infizierten Datei erscheint, wenn am SharePoint die Option ”Scan documents on download” aktiviert und die Option ”Allow users to download infected documents” deaktiviert ist:

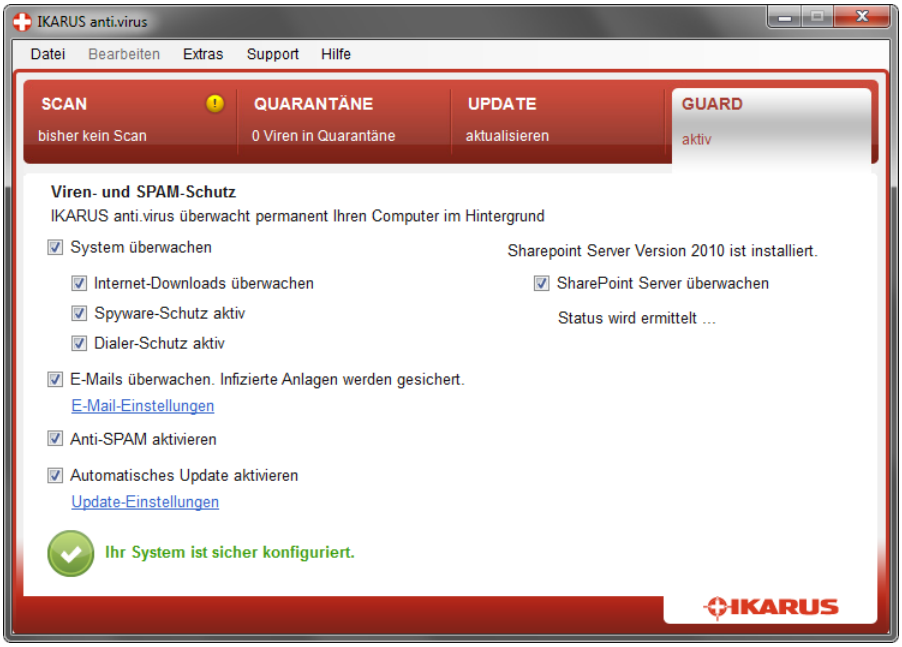

Error Found
"/Shared Documents/eicar.com.txt.11" contains the following error: "IKARUS anti.virus found: EICAR-ANTIVIRUS-TESTFILE".
If you want to open this file, you'll need to clean the file using your own scanning software. Do you want to save the file to your computer and attempt to clean it?

SharePoint stellt es dem Server-Administrator frei, das Scannen von Uploads und Downloads separat zu aktivieren oder zu deaktivieren. Wenn eine dieser beiden Optionen deaktiviert ist, führt also auch **IKARUS anti.virus** keine entsprechende Virenprüfung mehr durch. In der **IKARUS anti.virus**-Benutzeroberfläche wird der Status der beiden Optionen als Zusatzinformation angezeigt; geändert werden können sie jedoch nur direkt in der Administrationsoberfläche von SharePoint.

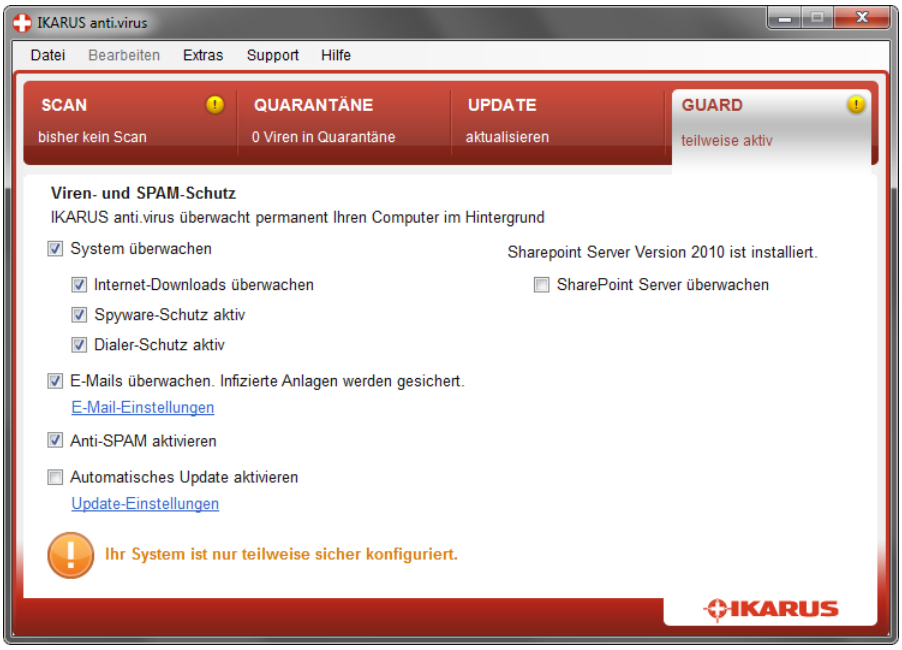
IKARUS anti.virus bietet die Möglichkeit, den SharePoint-Schutz komplett auszuschalten. In diesem Fall werden weder Uploads noch Downloads gescannt. Die folgende Abbildung zeigt das Häkchen mit der Beschriftung „SharePoint Server überwachen“, das Sie setzen oder entfernen können, um den SharePoint-Schutz zu steuern. Unter dem Häkchen wird der aktuelle Status von Upload- und Download-Scanning dargestellt:



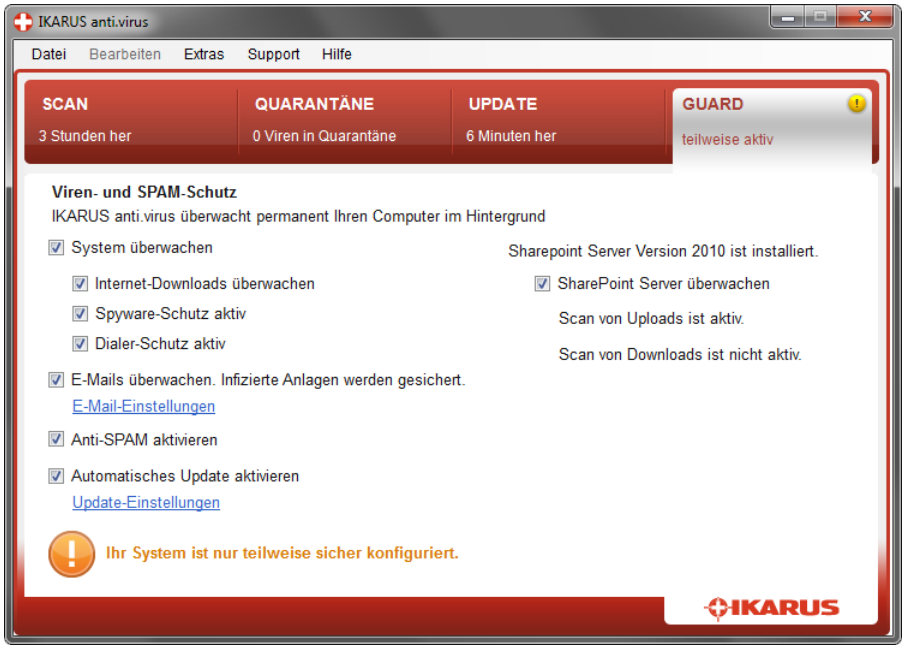
Es kann unter Umständen einige Augenblicke dauern, bis diese Einstellungen überprüft sind. In diesem Fall wird vorübergehend „Status wird ermittelt...“ angezeigt, wie in der folgenden Abbbildung ersichtlich:



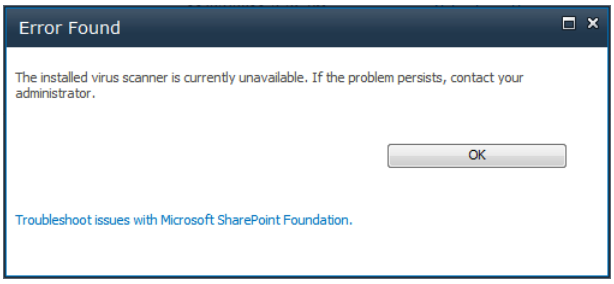
Die nächste Abbildung zeigt, dass bei deaktivierter SharePoint-Überwachung auch die Anzeigen von Upload- und Download-Status verschwinden. Damit ist der Systemschutz nicht mehr vollständig gegeben, was sich in der Anzeige des orangen Warnsymbols und dem Hinweis „Ihr System ist nur teilweise sicher konfiguriert“ äußert:



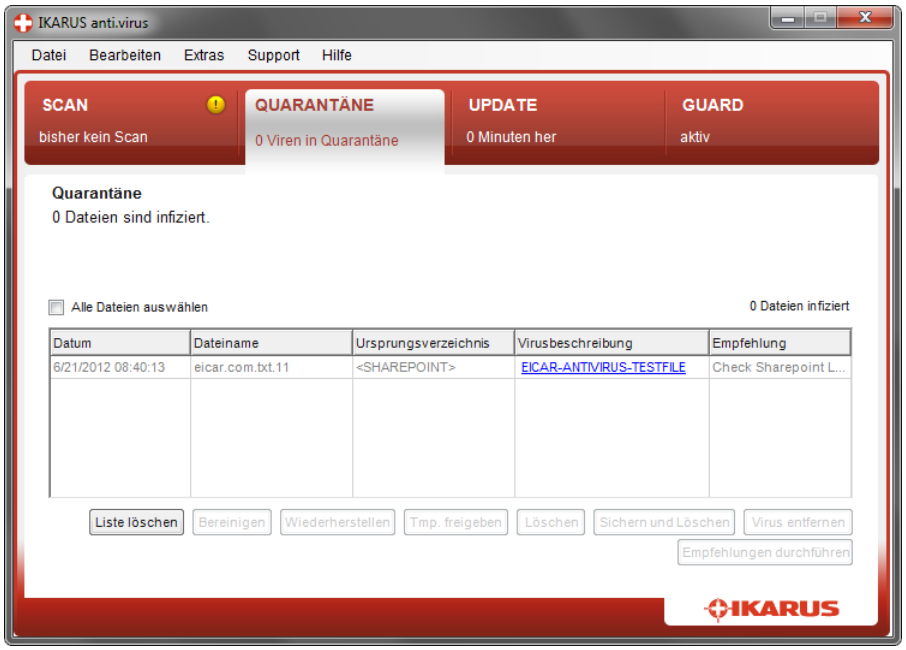
Derselbe Gesamtsystemstatus ist auch dann gegeben, wenn in der Administrationsoberfläche von SharePoint zumindest eine der beiden Optionen für Upload- oder Download-Scanning deaktiviert ist:



Sollten mit **IKARUS anti.virus** unerwartete Probleme auftreten, können keine SharePoint-Dateien gescannt werden. In diesem Fall werden aus Sicherheitsgründen der Upload und Download komplett unterbunden, sofern die jeweilige Scan-Option am SharePoint aktiviert ist. Für den SharePoint-Endbenutzer am Clientrechner äußert sich dieses Problem in folgender Fehlermeldung: „The installed virus scanner is currently unavailable. If the problem persists, contact your administrator."Die folgende Abbildung zeigt die Fehlermeldung im Webbrowser:


Error Found
The installed virus scanner is currently unavailable. If the problem persists, contact your administrator.
OK
Troubleshoot issues with Microsoft SharePoint Foundation.

Der SharePoint-Server erlaubt keinen direkten Zugriff auf die von ihm verwalteten Dokumente. Virenfunde durch das Plugin können daher nicht in die Quarantäne verschoben werden. In der Quarantäne-Ansicht von **IKARUS anti.virus** werden die infizierten Dateien jedoch als Hinweis für den Administator angezeigt.

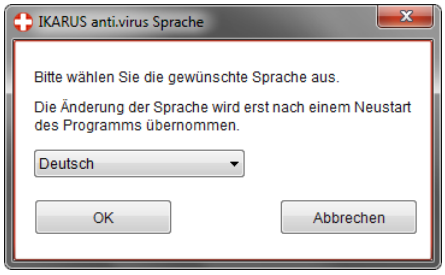


10 Einstellungen

10.1 Spracheinstellungen

IKARUS anti.virus kann in unterschiedlichen Sprachen verwendet werden. Bei der Installation wird die Sprache anhand der Einstellungen des PCs ermittelt.

Während des Betriebes können Sie die verwendete Sprache über den Menüpunkt ”Extras/Sprache” ändern.


IKARUS anti.virus Sprache
Bitte wählen Sie die gewünschte Sprache aus.
Die Änderung der Sprache wird erst nach einem Neustart des Programms übernommen.
Deutsch
OK
Abbrechen

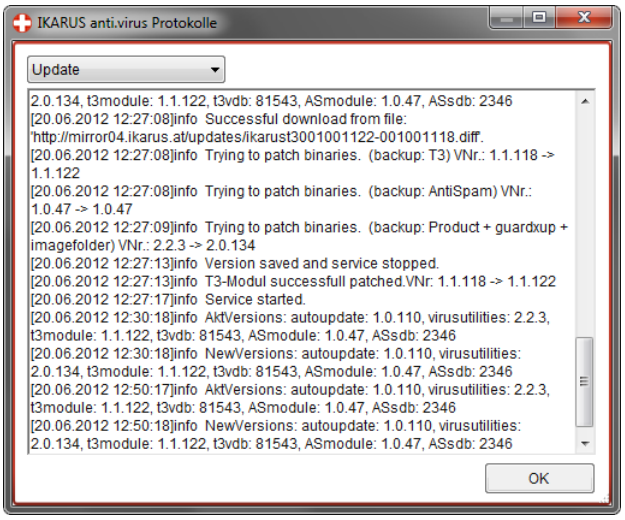
Nach einem Neustart von **IKARUS anti.virus** steht die Anzeige in dieser Sprache zur Verfügung.

Derzeit werden die folgenden Sprachen unterstützt:

- Chinesisch
- Deutsch
- Englisch
- Französisch
- Italienisch
- Spanisch

10.2 Protokolle

Im Menüpunkt ”Extras/Protokoll” können Sie auswählen, welche Protokolle von durchgeführten Aktionen Sie anzeigen wollen. Im Protokollfenster werden die letzten Aktionen von **IKARUS anti.virus** angezeigt.

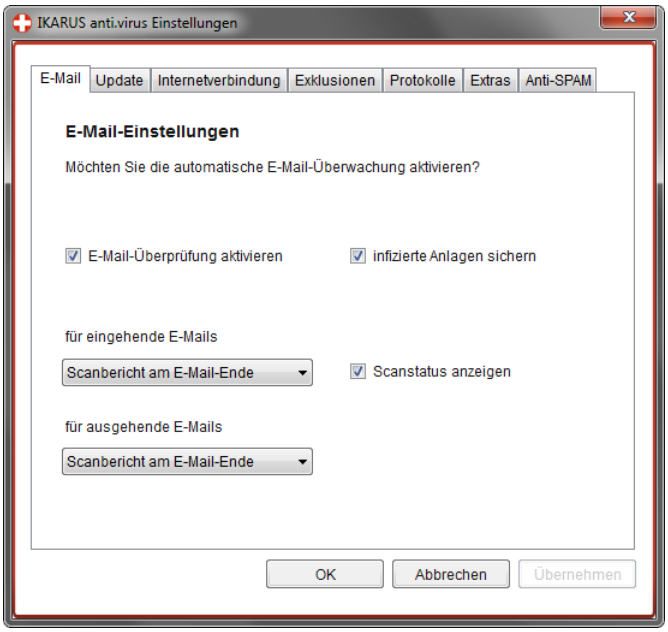

IKARUS anti.virus Protokolle
Update
2.0.134, t3module: 1.1.122, t3vdb: 81543, ASmodule: 1.0.47, ASsdb: 2346
[20.06.2012 12:27:08]info Successful download from file:
'http://mirror04.ikarus.at/updates/ikarust3001001122-001001118.diff'.
[20.06.2012 12:27:08]info Trying to patch binaries. (backup: T3) VNr.: 1.1.118 -> 1.1.122
[20.06.2012 12:27:08]info Trying to patch binaries. (backup: AntiSpam) VNr.: 1.0.47 -> 1.0.47
[20.06.2012 12:27:09]info Trying to patch binaries. (backup: Product + guardxup + imagefolder) VNr.: 2.2.3 -> 2.0.134
[20.06.2012 12:27:13]info Version saved and service stopped.
[20.06.2012 12:27:13]info T3-Modul successfull patched.VNr: 1.1.118 -> 1.1.122
[20.06.2012 12:27:17]info Service started.
[20.06.2012 12:30:18]info AktVersions: autoupdate: 1.0.110, virusutilities: 2.2.3, t3module: 1.1.122, t3vdb: 81543, ASmodule: 1.0.47, ASsdb: 2346
[20.06.2012 12:30:18]info NewVersions: autoupdate: 1.0.110, virusutilities: 2.0.134, t3module: 1.1.122, t3vdb: 81543, ASmodule: 1.0.47, ASsdb: 2346
[20.06.2012 12:50:17]info AktVersions: autoupdate: 1.0.110, virusutilities: 2.2.3, t3module: 1.1.122, t3vdb: 81543, ASmodule: 1.0.47, ASsdb: 2346
[20.06.2012 12:50:18]info NewVersions: autoupdate: 1.0.110, virusutilities: 2.0.134, t3module: 1.1.122, t3vdb: 81543, ASmodule: 1.0.47, ASsdb: 2346
OK

Diese Aufzeichnungen sind für Sie eine wesentliche Hilfestellung beim Kontakt mit der **IKARUS** Support-Hotline (siehe Abschnitt 11). Sie können auch selbst in den Protokollen nachsehen und überprüfen, welche Aktionen von **IKARUS anti.virus** durchgeführt wurden.

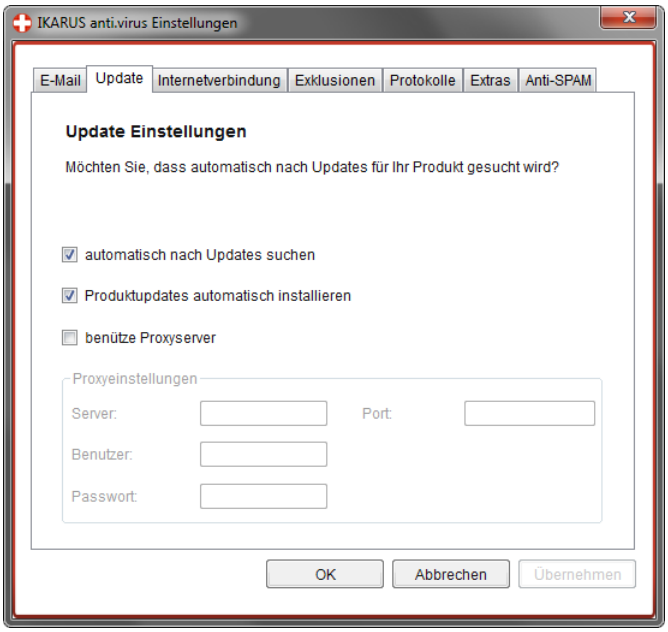
10.3 Einstellungen

IKARUS anti.virus bietet Ihnen im Menü ”Extras/Einstellungen” einen Dialog zur Konfiguration an. In dem Dialog sind die Einstellungsmöglichkeiten über Registrerkarten nach Themenberichen gegliedert.

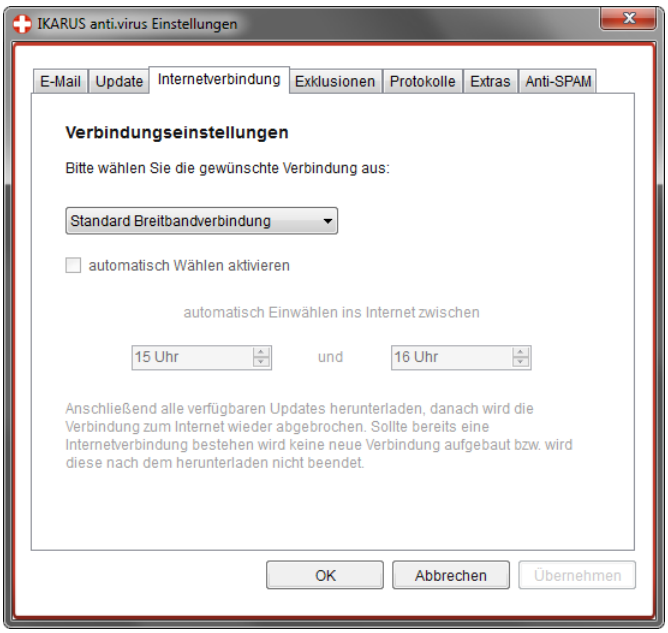
Auf der Registerkarte ”E-Mail” können Sie die E-Mail-Überwachung aktivieren und einstellen.



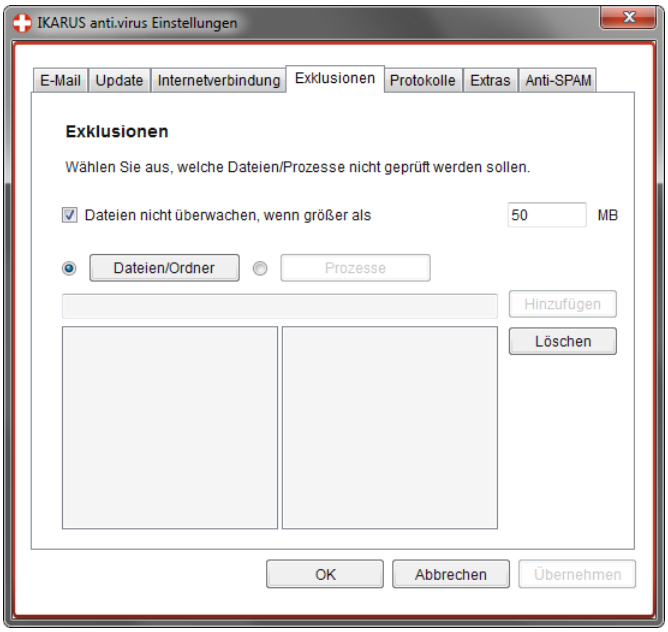
Die Registerkarte ”Update” zeigt Ihnen die verschiedenen Auswahlmöglichkeiten zum **IKARUS anti.virus**-Update.



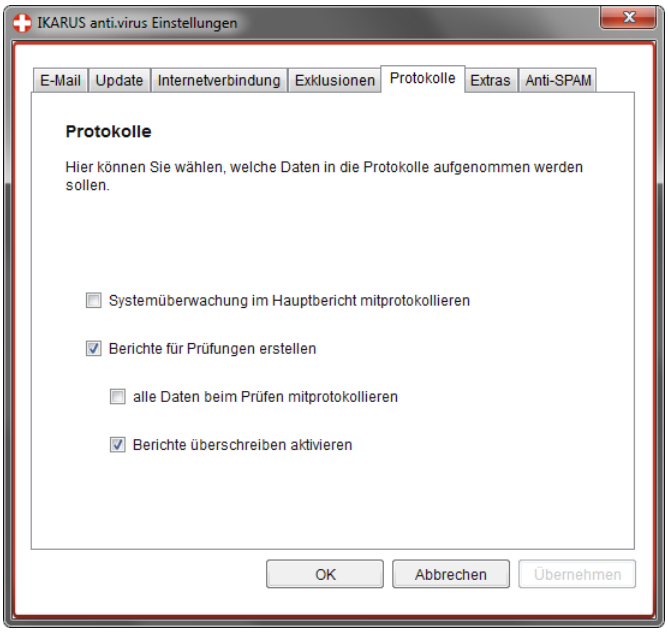
Auf dem Registerblatt ”Internetverbindung” stellen Sie die automatische Einwahl beim Update von **IKARUS anti.virus** ein. Hier können Sie einen Zeitraum auswählen, in welchem sich das AutoUpdate (bei Auswahl einer DFÜ-Verbindung) auch selbständig einwählen darf.



Auf der Registerkarte ”Exklusionen” können Sie auswählen, welche Dateien und Prozesse von der Prüfung durch **IKARUS anti.virus** ausgenommen sind. Diese Option kann für Sie von Vorteil sein, wenn Sie einen Dienst von der Prüfung ausnehmen wollen, der ohnedies schon genug Leistung Ihres PCs in Anspruch nimmt (MP3, Urlaubsfotos etc.), oder wenn ein Verzeichnis keinesfalls gescannt werden soll.



Auf der Registerkarte ”Protokolle” wählen Sie aus, welche Aktionen **IKARUS anti.virus** mitprotokollieren soll. So können Sie sicherstellen, dass die Systemüberwachung nach einer Deaktivierung wieder eingeschalten wird.



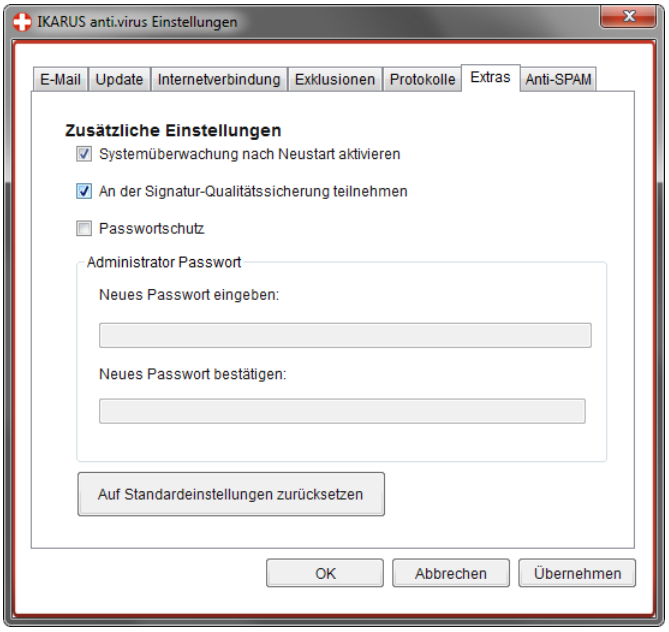
Auf der Registerkarte ”Extras” können Sie einige zusätzliche Einstellungen vornehmen.

- Es kann festgelegt werden, dass nach einem Neustart Ihres PCs die Systemüberwachung automatisch wieder aktiviert wird.
- Sie können an dem Programm zur Signatur-Qualitätssicherung teilnehmen. Dabei werden an IKARUS statistische Informationen zur Verbesserung der Virenerkennung auf Ihrem System übermittelt. Beachten Sie diesbezüglich die Lizenzbestimmungen im Abschnitt 12.3.

- Seit **IKARUS anti.virus** 2.2 besteht die Möglichkeit, einen Passwortschutz zu aktivieren. Ist dieser Schutz aktiviert, so können die Einstellungen von **IKARUS anti.virus** nur nach Eingabe des Passwortes geändert werden. Diese Option ist vor allem dann hilfreich, wenn Sie als Administrator eines Computers verhindern wollen, dass nichtberechtigte Benutzer Änderungen an den Einstellungen vornehmen.

  Dieser Passwortschutz gilt auch für das Aktivieren bzw. Deaktivieren der Systemüberwachung.

Mit dem Button ”Auf Standardeinstellungen zurücksetzen” werden alle Ihre Änderungen rückgängig gemacht und **IKARUS anti.virus** wird auf den Zustand nach der Installation zurückgesetzt.

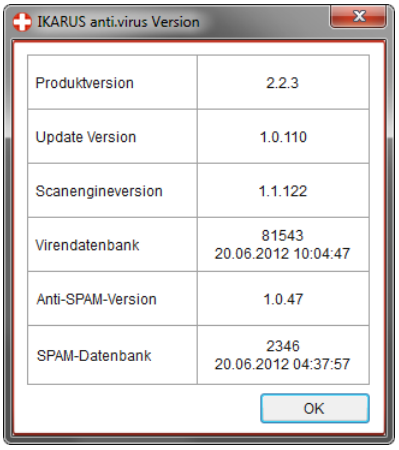


Auf der Registerkarte ”Anti-SPAM” finden Sie die Einstellungen für das **IKARUS anti.virus** Anti-SPAM-Modul. Weitere Informationen hierzu finden Sie unter dem Abschnitt Anti-SPAM.

11 Support

Für Anfragen und Rücksprache mit **IKARUS** ist es hilfreich, detaillierte Informationen über die beim Benutzer installierte Version von **IKARUS anti.virus** oder der Virendatenbank(VDB) zu erhalten.

Um die Kontaktaufnahme so effizient wie möglich anzubieten, haben wir mehrere Kontaktmöglichkeiten und Informationsübermittlungen in **IKARUS anti.virus** eingebaut.

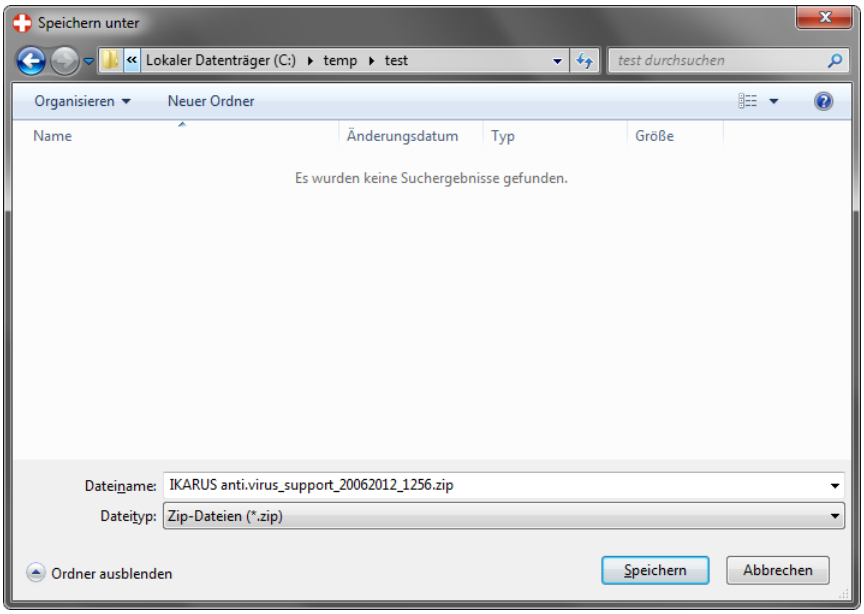


Über die Menüleiste „Support“ können Sie ganz einfach die aktuellen Versionsnummern von **IKARUS anti.virus** eruieren. Diese Angaben sind bei einem Kontakt mit unserem Supportteam wichtig!

Die Kontaktdaten selbst können Sie ebenfalls einfach über **IKARUS anti.virus** aufrufen.

Wenn Sie uns über diesen Link eine E-Mail schicken, wird diese automatisch mit den wichtigsten Versionsinformationen ergänzt.

Unter dem Menüpunkt ”Support” - ”Support Info speichern” können Sie auf einen Klick die wichtigsten Supportinfos zusammenfassen und uns in Form eines ZIP-Files leicht übermitteln.

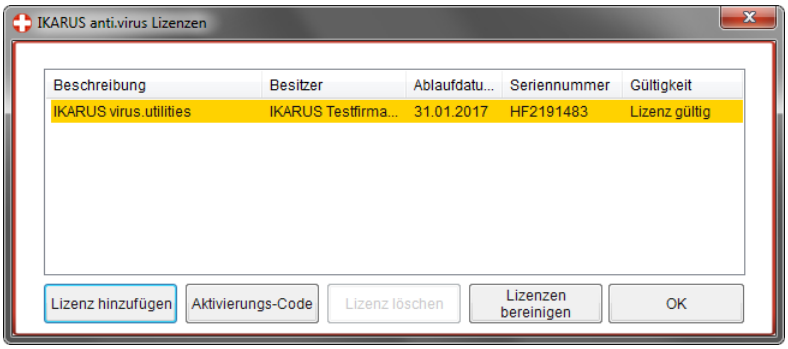


11.1 Lizenzschlüssel

Die Verwendung von **IKARUS anti.virus** wird über den Lizenzschlüssel aktiviert. Dieser Schlüssel regelt die Dauer der Verwendung sowie die Anzahl der Benutzer.

Sie erhalten diesen Schlüssel beim Kauf bzw. bei der Registierung mittels Aktivierungscode in Form einer Lizenzdatei.

Über den Menüpunkt ”Hilfe/Lizenzschlüssel” können Sie Ihre Lizenzschlüssel überprüfen, löschen, hinzufügen und archivieren.



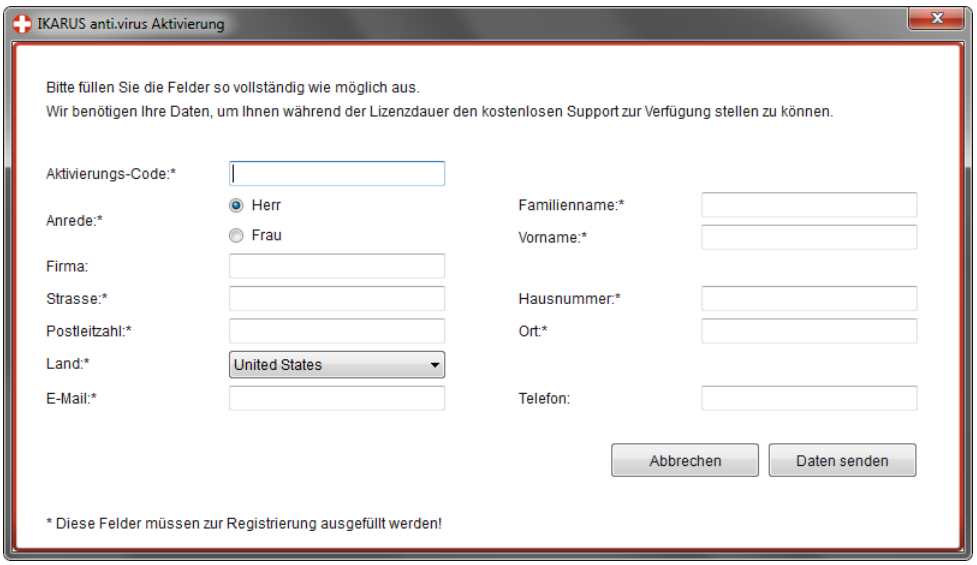
Es können auch mehrere Lizenzschlüssel gleichzeitig verwaltet werden, z.B. wenn ein Lizenzschlüssel in Kürze ausläuft und Sie bereits einen neuen erhalten haben.

IKARUS anti.virus wählt automatisch den richtigen Schlüssel aus.

Bitte kontaktieren Sie unseren Support, wenn Sie Ihren Lizenzschlüssel nicht mehr finden oder keinen erhalten haben.

Wenn Sie einen Aktivierungscode besitzen, haben Sie hier die Möglichkeit, sich damit zu registrieren und einen

Lizenzschlüssel vollautomatisch in das Programm integrieren zu lassen.



12 Anhang

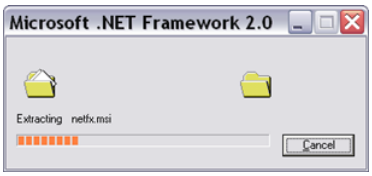
Hier erhalten sie Informationen über die Installation des Microsoft NET Framework, die Konfiguration von Firewalls und die lizenzrechtlichen Bestimmungen der **IKARUS Security Software GmbH**.

12.1 .NET Framework

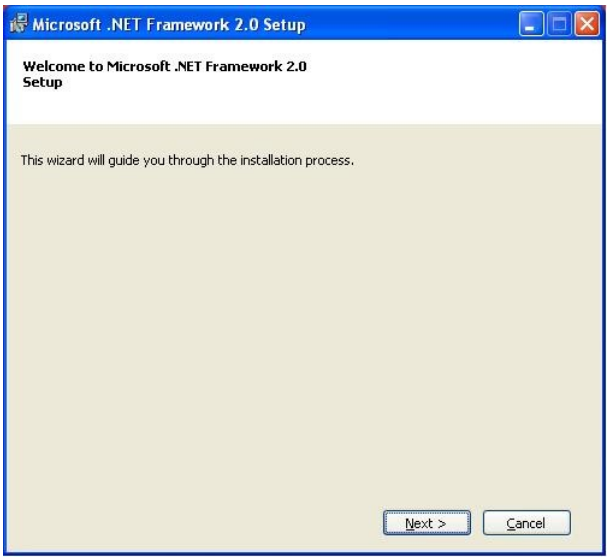
.NET Framework wird benötigt, um die graphische Oberfläche von **IKARUS anti.virus** darstellen zu können. Wenn Sie .NET Framework bereits auf Ihrem Computer installiert haben, wird die Installation von **IKARUS anti.virus** ohne Unterbrechung abgeschlossen. Ist auf Ihrem PC noch kein .NET Framework gespeichert, wird dieses entweder automatisch von der Installations-CD nachinstalliert oder, falls Sie nicht von einer CD installieren, von der Microsoft Webseite heruntergeladen.

.NET Framework ist eine Freeware-Version von Microsoft. Sie müssen dafür also keinerlei Lizenzkosten bezahlen und keine Registrierung durchführen.

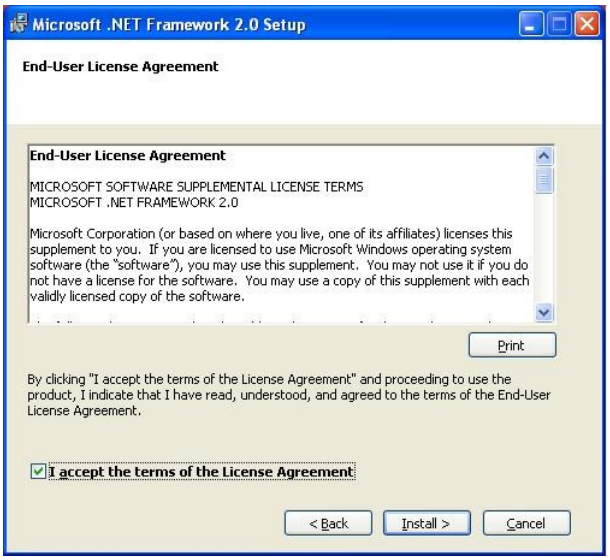
Folgendes Fenster wird Ihnen vom Setup angezeigt, wenn Sie noch kein .NET Framework auf Ihrem Computer installiert haben:

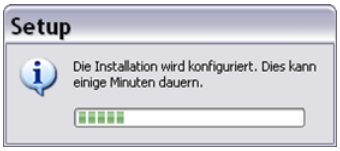


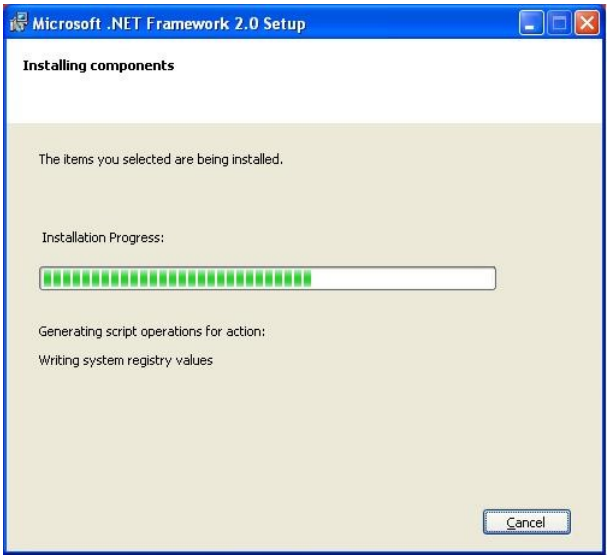
Entweder startet sich nach einem Klick auf OK der Download des .NET Framework, oder, wenn Sie von CD installieren, gleich das Setup. Nachdem die Dateien vom .NET Framework Setup geladen sind werden Sie mit nachfolgendem Fenster begrüßt. Klicken Sie auf ”Weiter” um zum Endbenutzer-Lizenzvertrag zu gelangen.

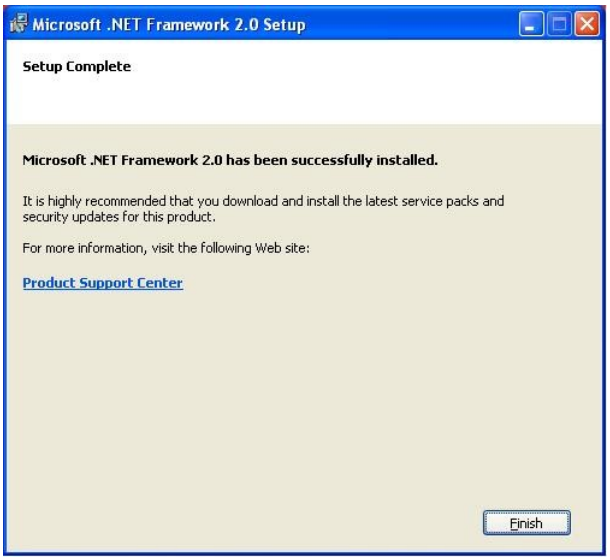

Microsoft .NET Framework 2.0 Setup
Welcome to Microsoft .NET Framework 2.0 Setup
This wizard will guide you through the installation process.
Next >
Cancel

Nachdem Sie dem Lizenzvertrag zugestimmt haben, starten Sie mit einem Klick auf ”Installieren” die Installation.


Microsoft .NET Framework 2.0 Setup
End-User License Agreement
End-User License Agreement
MICROSOFT SOFTWARE SUPPLEMENTAL LICENSE TERMS
MICROSOFT .NET FRAMEWORK 2.0
Microsoft Corporation (or based on where you live, one of its affiliates) licenses this supplement to you. If you are licensed to use Microsoft Windows operating system software (the "software"), you may use this supplement. You may not use it if you do not have a license for the software. You may use a copy of this supplement with each validly licensed copy of the software.
Print
By clicking "I accept the terms of the License Agreement" and proceeding to use the product, I indicate that I have read, understood, and agreed to the terms of the End-User License Agreement.
I accept the terms of the License Agreement
< Back
Install >
Cancel


Setup
Die Installation wird konfiguriert. Dies kann einige Minuten dauern.


Microsoft .NET Framework 2.0 Setup
Installing components
The items you selected are being installed.
Installation Progress:
Generating script operations for action:
Writing system registry values
Cancel


Microsoft .NET Framework 2.0 Setup
Setup Complete
Microsoft .NET Framework 2.0 has been successfully installed.
It is highly recommended that you download and install the latest service packs and security updates for this product.
For more information, visit the following Web site:
Product Support Center
Finish

Nach erfolgter Installation beenden Sie das Setup von .NET Framework mit einem Klick auf ”Fertig stellen”.

12.2 Personal Firewall

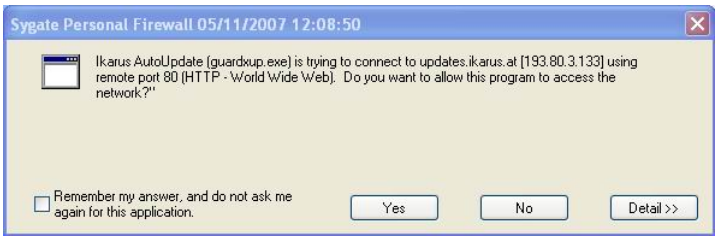
Um die Effizienz des Virenscanners jederzeit aufrecht zu erhalten, sind immer wieder Updates aus dem Internet notwendig. Sei es, um die Virendatenbanken auf dem neuesten Stand zu halten, oder um **IKARUS anti.virus** um neue Funktionen erweitern zu können.

Viele Computer werden zusätzlich durch eine Personal Firewall abgesichert, die Sie vor Angriffen aus dem Internet schützt. Damit das Updateprogramm von **IKARUS anti.virus** auf die Updateserver im Internet zugreifen kann, muss es bei der Personal Firewall angemeldet werden.

Wir zeigen Ihnen drei Beispiele, wie Sie Ihre Firewall entsprechend anpassen können:

Sygate

In diesem Fenster werden Sie darauf hingewiesen, dass ”IKARUS AutoUpdate” auf das Internet zugreifen will. Aktivieren Sie die Checkbox ”An meine Antwort erinnern. . . ” und klicken Sie anschließend auf den Button ”Ja”.


Sygate Personal Firewall 05/11/2007 12:08:50
Ikarus AutoUpdate (guardxup.exe) is trying to connect to updates.ikarus.at [193.80.3.133] using remote port 80 (HTTP - World Wide Web). Do you want to allow this program to access the network?'
Remember my answer, and do not ask me again for this application.
Yes
No
Detail >>

Ab diesem Zeitpunkt ist ”GuardX Update” bei der Firewall angemeldet und kann jederzeit nach neuen Updates suchen.

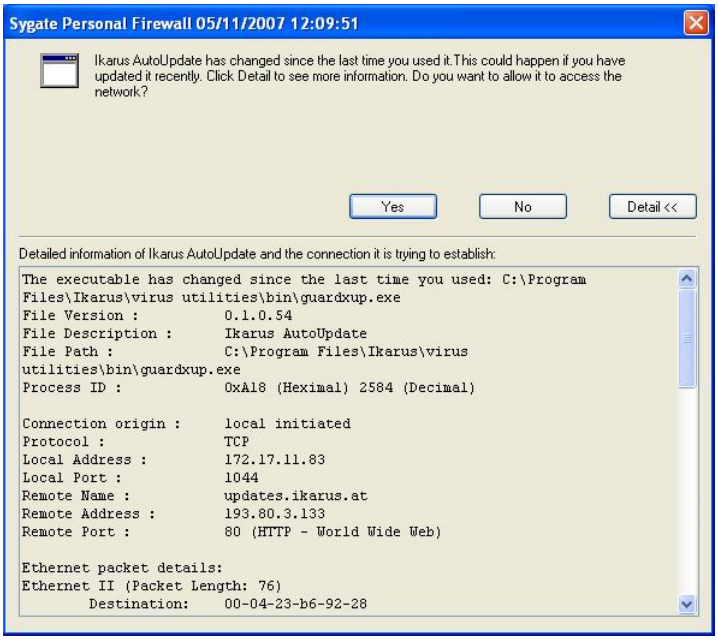
ZoneAlarm

In diesem Fenster werden Sie darauf hingewiesen, dass ”IKARUS AutoUpdate” auf das Internet zugreifen will. Aktivieren Sie die Checkbox ”Remember this setting” und klicken Sie anschließend auf den Button ”Allow”.

Ab diesem Zeitpunkt ist ”GuardX Update” bei der Firewall angemeldet und kann jederzeit nach neuen Updates suchen.

Wird das ”IKARUS AutoUpdate” selbst upgedated, muss es bei der Firewall neu angemeldet werden. Die sieht dann folgendermaßen aus:

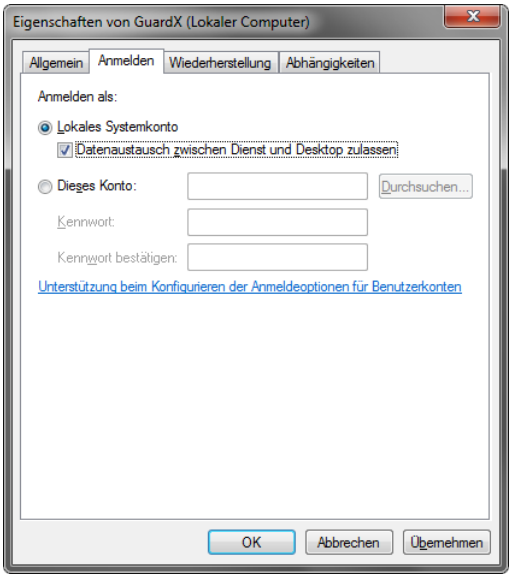
Sygate: Bestätigen Sie die Neuanmeldung mit Klick auf den Button ”Ja”.


Sygate Personal Firewall 05/11/2007 12:09:51
Ikarus AutoUpdate has changed since the last time you used it.This could happen if you have updated it recently. Click Detail to see more information. Do you want to allow it to access the network?
Yes
No
Detail <<
Detailed information of Ikarus AutoUpdate and the connection it is trying to establish:
The executable has changed since the last time you used: C:\Program Files\Ikarus\virus utilities\bin\guardxup.exe
File Version : 0.1.0.54
File Description : Ikarus AutoUpdate
File Path : C:\Program Files\Ikarus\virus utilities\bin\guardxup.exe
Process ID : 0xA18 (Heximal) 2584 (Decimal)
Connection origin : local initiated
Protocol : TCP
Local Address : 172.17.11.83
Local Port : 1044
Remote Name : updates.ikarus.at
Remote Address : 193.80.3.133
Remote Port : 80 (HTTP - World Wide Web)
Ethernet packet details:
Ethernet II (Packet Length: 76)
Destination: 00-04-23-b6-92-28

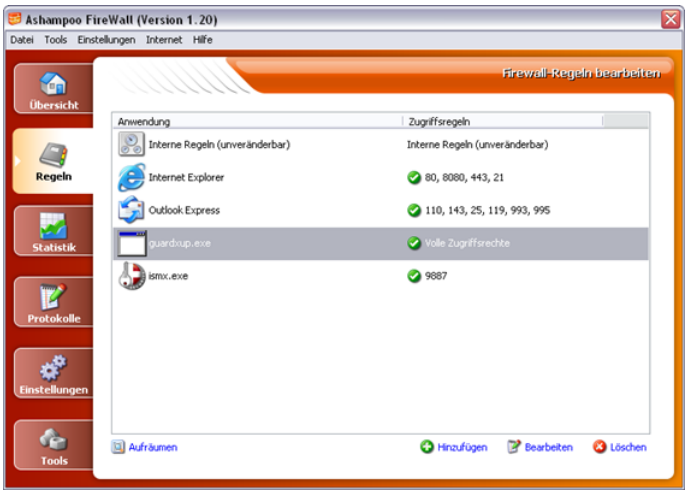
ZoneAlarm: Bestätigen Sie die Neuanmeldung durch aktivieren der Checkbox ”Remember this setting” und anschließendem Klick auf den Button ”Allow”.

Ashampoo

Hier muss bei der Verwaltung des Dienstes ”GuardX” im Abschnitt ”Anmelden” die Einstellung ”Datenaustausch zwischen Dienst und Desktop zulassen” aktiviert werden:



Anschließend kann in der Firewall die Regel für die ”guardxup.exe” erstellt werden.



Damit steht Ihnen das automatische Update zur Verfügung.

12.3 Lizenzrechtliche Bestimmungen

IKARUS SECURITY SOFTWARE LIZENZ- UND WARTUNGSVERTRAG

Lesen Sie bitte diese Vereinbarung sorgfältig durch! Mit Installierung der gelieferten Software anerkennen Sie die untenstehenden Lizenzbedingungen. Sollten Sie damit nicht einverstanden sein, brechen Sie den Installationsvorgang ab und nehmen Sie von der weiteren Verwendung der gelieferten Software Abstand. Eine Verletzung dieser Lizenzbedingungen kann eine Urheberrechtsverletzung sein, die zivil- und strafrechtlich verfolgt wird.

1. Lizenz
Lizenzgeber ist die IKARUS Security Software GmbH. Gegenstand dieses Lizenzvertrages ist die Einräumung einer nicht übertragbaren und nicht ausschließlichen Nutzungsbewilligung für die auf den Datenträgern aufgezeichneten Computerprogramme samt Programmbeschreibung, Bedienungsanleitung und Dokumentation an Sie, den Lizenznehmer. Der Einfachheit halber nennen wir das gesamte Paket im weiteren ”Software”.

1.1. Die Bestimmungen dieser Vereinbarung gelten auch für zukünftig ausgefolgte Updates für die Software. Mit Zustandekommen dieses Lizenzvertrages vereinbaren Sie somit auch einen Wartungsvertrag, durch den Sie regelmäßige Updates der gelieferten Software erhalten.

2. Umfang der Lizenz
2.1. Die Software darf nur für die Dauer dieses Vertrages und nur auf einem einzelnen Computersystem (einer zentralen Recheneinheit) und an einem einzigen Ort benützt werden. Die Benützung der Software in Netzwerken oder auf mehreren PCs darf nur mit zusätzlich hiefür erworbenen Netzwerk- oder Mehrplatzlizenzen erfolgen, die auf die Anzahl der PC ausgestellt wurde, auf denen diese zur Anwendung kommen. Sollten Sie hierüber nicht verfügen, ist mit uns das Einvernehmen herzustellen und die erforderliche Anzahl von Zusatzlizenzen zu erwerben. Eine gleichzeitige Übertragung der Software auf andere Rechner ist unzulässig. Insbesondere ist es unzulässig, die für einen Einzelplatz oder für Mehrplätze lizensierte Software Dritten in irgendeiner Weise zugänglich zu machen und/oder entgeltlich oder unentgeltlich zur (Be-)Nutzung direkt oder indirekt zur Verfügung zu stellen. Im Besonderen ist auch jede Nutzung der Software auf Servern unzulässig, sofern dies zur Überprüfung auf Viren etc. des Datenverkehrs von Dritten, seien es auch Vertragspartner des Lizenznehmers (z.B. Access-Kunden, Mailbox-Kunden), dient. Eine Benutzung der Software für diese Zwecke bedarf der ausdrücklichen schriftlichen Vereinbarung mit der Lizenzgeberin. Soweit in diesem Lizenz- und Wartungsvertrag von Computersystemen und PCs die Rede ist, gelten die Bestimmungen sinngemäß auch für die Verwendung der Software in sonstigen Recheneinheiten wie beispielsweise Mobiltelefonen.

2.2. DVDs, CDs oder sonstige Kopien der Software dürfen nicht weitergegeben werden, auch nicht zu privaten Zwecken, es sei denn, wir stimmen dieser Weitergabe ausdrücklich schriftlich zu. Ohne schriftliche Einwilligung von uns darf die Software – mit Ausnahme gesetzlich zwingend zulässiger Eingriffe – weder dekompiliert, zurückentwickelt, disassembliert noch in sonstiger Art und Weise in eine für Menschen wahrnehmbare Form gebracht werden. Weiters darf die Software ohne schriftliche Einwilligung von uns nicht modifiziert, adaptiert, übersetzt, verkauft oder Dritten auf sonstige Weise unentgeltlich oder gegen Bezahlung zum Gebrauch überlassen werden, soweit dies nicht nach dieser Vereinbarung oder zwingenden gesetzlichen Vorschriften gestattet ist.

3. Gewährleistung
3.1. Wir leisten Gewähr dafür, dass die Software im Sinne der Dokumentation nach dem Stand der Technik zum Zeitpunkt der Lieferung mängelfrei und grundsätzlich brauchbar ist, ohne jedoch allen denkbaren Anwendungsbedingungen zu genügen. Sie nehmen zustimmend zur Kenntnis , dass nach dem derzeitigen Stand der Technik keine Entwicklung von fehlerfreier Software möglich ist. Dies gilt in besonderem Maße für das Gebiet der Virenbekämpfung, wo ständig neue Viren, Trojaner, Würmer und vergleichbare Programme entstehen, die zum Teil speziell zur Umgehung von Virenschutzprogrammen spezialisiert werden.

3.2. Wir leisten daher weder Gewähr dafür, dass die Software allen Ihren Anforderungen, noch dass die in der Software enthaltenen Funktionen ununterbrochen und fehlerfrei in allen von Ihnen gewünschten Kombinationen mit beliebigen Daten, Programmen und EDV-Systemen eingesetzt werden kann, noch dass durch die Korrektur von Softwarefehlern das Auftreten anderer Softwarefehler ausgeschlossen wird. Auch übernehmen wir keine Gewähr für Fehler, Störungen oder Schäden, die auf unsachgemäße Bedienung, Transportschäden, Betriebssystemfehler, geänderte Betriebssystemkomponenten, Schnittstellen und Parameter oder Verwendung ungeeigneter Organisationsmittel und Datenträger zurückzuführen sind.

3.3. Die Gewährleistung erlischt, wenn ohne unsere schriftliche Einwilligung Sie selbst oder ein Dritter an der Software Änderungen oder Instandsetzungen vornimmt. Wir können auch Aufwendungen in diesem Zusammenhang nicht anerkennen. Für Software, die geändert, erweitert oder beschädigt, oder die unter anderen als den vertraglich vereinbarten Nutzungsbedingungen eingesetzt wurde, übernehmen wir keinerlei Gewähr, es sei denn, dass die Änderung, Erweiterung oder Beschädigung für den Mangel nicht ursächlich war.

3.4. Allfällige Mängel der Software sind uns längstens binnen acht Tagen – bei Verbrauchern jedoch innerhalb der gesetzlichen Fristen – nach Erkennbarkeit schriftlich mitzuteilen, andernfalls die Gewährleistung erlischt. Die Gewährleistungsfrist beträgt einvernehmlich für Verbraucher zwei Jahre, ansonsten sechs Monate.

4. Schadenersatzansprüche
4.1. Schadenersatzansprüche gegen uns sind ausgeschlossen, soweit nicht in Fällen des Vorsatzes oder der groben Fahrlässigkeit gesetzlich zwingend die Haftung eintritt. Der Haftungsausschluss bezieht sich insbesondere auch auf Schäden durch Viren oder vergleichbare Programme, da eine absolut wirksame Virenbekämpfung nach dem Stand der Technik unmöglich ist. Die Haftung für Folgeschäden einschließlich des Gewinnentganges und für mittelbare Schäden ist jedenfalls ausgeschlossen. Weiters ist jede Haftung von uns für Schäden, die durch unberechtigte Eingriffe Dritter entstehen, ebenso ausgeschlossen, wie die Haftung für mangelhafte Bedienung oder Installation.

4.2. Es wird Ihnen ausdrücklich empfohlen, regelmäßig Sicherungskopien von den auf Ihren Computern befindlichen Daten anzufertigen. Sofern Sie dieser Schadensminderungspflicht nicht nachkommen, haften wir nicht für infolge dieses Verstoßes entstandene Schäden. Diese Schadensbegrenzung gilt nicht, wenn das schadenauslösende Ereignis durch uns grob fahrlässig oder vorsätzlich verursacht wurde; jedoch ist auch dann bei der Ersatzbemessung die fehlende Sicherungskopie als Mitverschulden zu berücksichtigen.

5. Beginn und Dauer des Lizenzvertrages
5.1. Dieser Vertrag kommt mit Willensübereinstimmung zwischen Ihnen und uns, spätestens aber durch die von Ihnen vorgenommene tatsächliche Installation dieser Software auf einem PC zu Stande. Eine ausdrückliche Willensübereinstimmung kann schriftlich, per Post, per E-Mail oder auch durch persönliche Abholung oder Zustellung erklärt werden.

5.2. Dieser Vertrag läuft für die ursprünglich zwischen Ihnen und uns gemäß gesonderter Vereinbarung (siehe Rechnung) vereinbarte Mindestlaufzeit. Er verlängert sich nach deren Ablauf jeweils um diese Laufzeit. Während der Vertragslaufzeit werden wir die Ihnen gelieferte Software ständig verbessern, warten und auf den neuesten Stand bringen. Insbesondere werden wir dafür sorgen, dass die Software auch ihr bisher unbekannte Viren udgl. erkennt. Die erforderlichen Programmupdates werden wir Ihnen an die uns zuletzt bekannt gegebene Adresse zusenden. Außerdem steht Ihnen unsere Virendatenbank für online Updates zur Verfügung. Sollte es aufgrund der technischen Entwicklungen erforderlich sein, das bestehende Lizenzprodukt komplett auszuwechseln, übermitteln wir Ihnen die erforderliche Software zur Neuinstallation. Unser Supportcenter steht Ihnen in diesen Fällen zur Verfügung

5.3. Für die eingeräumte Lizenz sowie das aufgrund der Wartungsvereinbarung regelmäßig durchgeführte Update wird ein Entgelt vereinbart. Wir behalten uns Preisänderungen vor. Sie haben das Recht, im Falle der Bekanntgabe einer Preiserhöhung unter Einhaltung der vertraglichen Kündigungsfristen das Vertragsverhältnis aufzukündigen.

5.4. Dieser Vertrag läuft für mindestens die von Ihnen gewählte Lizenzdauer und verlängert sich sodann nach Ablauf jeweils wieder um diese Lizenzdauer, sofern er nicht innerhalb von 14 Tagen nach Erhalt der Rechnung für den neuen Lizenzzeitraum gekündigt wird. Verbraucher haben das Recht, diesen Vertrag unter Einhaltung der Kündigungsfrist zum Ende des ersten Vertragsjahres und sodann jedes halbe Vertragsjahr zu kündigen. Mit Ablauf des Vertragsverhältnisses ist die weitere Nutzung der Software unzulässig. Sie sind in diesem Falle verpflichtet die Originaldatenträger samt allen Kopien und Unterlagen zu vernichten. Eine weitere Nutzung der Software über den Vertragsbeendigungstag hinaus stellt eine Urheberrechtsverletzung dar.

5.5. Sollten Sie gegen eine Bestimmung dieser Vereinbarung, insbesondere in Bezug auf den Umfang der Ihnen eingeräumten Rechte, verstoßen, so sind wir berechtigt, unverzüglich diesen Vertrag mit sofortiger Wirkung zu beenden. Auch in diesem Fall ist jede weitere Nutzung der Software unzulässig.

6. Qualitätssicherung
6.1. Sie können ab sofort an unserem Programm zur Signatur-Qualitätssicherung teilnehmen. Sie übermitteln IKARUS statistische Informationen zur Verbesserung der Virenerkennung auf Ihrem System. Dabei können auch infizierte Dateien von Ihrem System an IKARUS für eine Analyse übermittelt werden. Wenn Sie nicht an der Signatur-Qualitätssicherung teilnehmen wollen, so können Sie die Teilnahme in den Einstellungen deaktivieren. Bitte beachten Sie: Im Zuge dieser Maßnahme werden von IKARUS keine personenbezogenen Daten verarbeitet.

7. Schlussbestimmungen
7.1. Auf diese Vereinbarung ist österreichisches Recht unter Ausschluss des UN-Kaufrechts anwendbar. Gerichtsstand für sämtliche Streitigkeiten aus dieser Vereinbarung und anlässlich ihrer Beendigung ist das zuständige Gericht für Handelssachen in Wien, sind Sie aber Verbraucher, Ihr allgemeiner Gerichtsstand. Änderungen und Ergänzungen dieser Vereinbarung bedürfen ihrer Rechtsgültigkeit der Schriftform und der rechtsverbindlichen Unterzeichnung durch die Vertragspartner; dies gilt auch für das Abgehen von dieser Formvorschrift.

Wenn Sie mit den Bedingungen dieser Lizenzvereinbarung nicht einverstanden sind, kommt ein Vertrag zwischen uns nicht zustande und dürfen Sie die Software weder installieren noch in Betrieb nehmen. Führen Sie dennoch eine Installation und/oder Inbetriebnahme durch, so erklären Sie damit Ihr Einverständnis mit den Lizenzbedingungen. Wollen Sie diesen Vertrag kündigen, so ersuchen wir Sie um Kontaktaufnahme.